CHAPTER

13

MANAGING INTERNET AND NETWORK INTEROPERABILITY

After reading this chapter and completing the exercises you will be able to:

- Install and configure a Web server and a Media Services server
- Install and configure DNS and WINS servers
- Install and configure a DHCP server
- Install and configure a terminal server
- Configure a Telnet server
- Install and configure a NetWare gateway

Microsoft Windows 2000 Server is capable of providing a large range of specialized connectivity services, including Web services, operating as DNS/WINS or DHCP servers, and functioning as terminal or Telnet servers. Operating as a Web server is one of the most popular functions for a Windows 2000 server, because Web servers are used all over the world for e-mail communications, selling goods and services, disseminating information, advancing scientific research, and a wide range of other uses. DNS/WINS and DHCP servers provide vital behind-the-scenes functions on networks by translating computer names to IP addresses and by automatically assigning IP addresses. Terminal servers enable companies to save money by using low-cost computers with minimal operating system functions to access the resources of a Windows 2000 server. Configuring Windows 2000 Server as a Telnet server is a way to enable clients without Windows operating systems to access a server. Also, Windows 2000 Server can be configured as a NetWare gateway to enable users to access a NetWare server's directories and printers without directly connecting to NetWare as a client.

In this chapter, you first learn how to set up Windows 2000 Server to operate as a Web server. Next, you learn how to set up DNS, WINS, and DHCP servers. Finally, you learn how to configure terminal services, a Telnet server, and a NetWare gateway.

To configure any of these services you must have Administrator privileges.

Microsoft Internet Information Services

Microsoft **Internet Information Services** (**IIS**) is a component included on the Windows 2000 Server CD-ROM that enables you to offer a complete Web site from a Windows 2000 server. Your Web site might fulfill any number of functions. On a college campus you might use it to enable applicants to apply for admission, or to allow currently enrolled students to view their progress toward completing degree requirements. Many companies use their Web sites for multiple purposes such as to announce new products, provide product support, take product orders, and advertise job openings. Another use is providing training to company employees on using software such as an inventory or order entry system.

IIS benchmarks prove that these services are fast, and the software design enables the use of extensions to link other software applications to an IIS server, such as a distributed client/server system that implements Web-based features. One reason why IIS services are fast and can be integrated with other programs is the built-in **Internet Server Application Programming Interface** (**ISAPI**). ISAPI is a group of DLL (dynamic-link library) files that are applications and filters. The application files enable developers to link customized programs into IIS and to speed up program execution. IIS filters are used to automatically trigger programs, such as a Microsoft Access database lookup or a security program that authorizes user access to specific Web functions. The IIS component contains two critical services for a Web site: World Wide Web and FTP. The World Wide Web (Web or WWW) is a series of file servers with software such as Microsoft IIS that make HTML and other Web documents available for workstations. HTML files are read by Internet, intranet, and VPN users with the help of client software called a **Web browser**, such as Netscape Communicator and Microsoft Internet Explorer. FTP is a TCP/IP-based application protocol that handles file transfers over a network (see Chapter 3). Also, there are additional services that you can install to make an IIS server function as an e-mail server using the Simple Mail Transfer Protocol (SMTP, see Chapter 3) and as a **Network News Transfer Protocol** (**NNTP**) server. An SMTP server acts as an Internet gateway in partnership with e-mail services, such as Microsoft Exchange, to accept incoming e-mail from the Internet and forward it to the recipient. It also forwards outgoing e-mail from a network's e-mail service to the Internet. NNTP is used over TCP/IP-based networks by NNTP servers to transfer news and informational messages to client subscribers who compose "newsgroups."

There are several reasons why Windows 2000 Server makes a good candidate as a Web server. One reason is that the Windows 2000 Server privileged-mode architecture (see Chapter 1) and fault-tolerance capabilities (see Chapter 7) make it a reliable server platform. Another reason is that Windows 2000 Server is compatible with small databases, such as Microsoft Access, and large databases, such as SQL Server and Oracle. Also, users can log directly into a database through the IIS **Open Database Connectivity** (**ODBC**) drivers. ODBC is a set of rules developed by Microsoft for accessing databases and providing a standard doorway to database

data. This makes IIS very compatible with Web-based client/server applications. IIS also is compatible with MPPE security (see Chapter 12), IPSec, and the **Secure Sockets Layer (SSL)** encryption technique (Chapter 4). SSL is a dual-key encryption standard for communication between a server and a client and is also used by Internet Explorer. IIS enables security control on the basis of username and password, IP address, and folder and file access controls.

Installing a Web Server

There are several requirements for installing and using IIS:

- Windows 2000 Server installed on the computer to host IIS
- TCP/IP installed on the IIS host
- Access to an Internet service provider (ISP)—ask the ISP for your IP address, subnet mask, and default gateway IP address
- Sufficient disk space for IIS and for Web site files (the required space depends on the number of Web files that you publish)
- Disk storage formatted for NTFS (IIS can run on FAT, but NTFS has better performance and security)
- A method for resolving computer and domain names to IP addresses, such as DNS and WINS

You can install IIS when you install Windows 2000 Server, which is the default installation method. When the Windows 2000 Server Setup displays the list of components that can be installed, IIS is automatically checked as one of those components (see Chapter 5). If you do not install IIS during the Windows 2000 installation, you can install it later by using the Control Panel Add/Remove Programs icon. After you open the icon, click Add/Remove Windows Components, click the Components button (if necessary) to start the Windows Components Wizard, and select the option to install Internet Information Services in the Windows Components dialog box (try Hands-on Project 13-1). Another way to install IIS and to configure the IIS services is to:

1. Click Start, point to Programs, point to Administrative Tools, and click Configure Your Server.
2. Click the Web/Media Server hyperlink in the menu on the left side of the window, and then click Web Server.
3. Click the Start hyperlink to access the Windows Components dialog box.
4. Scroll to Internet Information Services (IIS) and double-click that option.
5. Make sure all of the services that you want to install are checked in the Internet Information Services (IIS) dialog box (see Figure 13-1 and Table 13-1). Click any box to place a check in it or to remove a check. Click any of the service names to view a description of it. Double-click service names that have their own subcomponents from which to select, and check the subcomponents that you want to install. Click OK on all dialog boxes that you have opened and configured, until you return to the Windows Components Wizard dialog box.

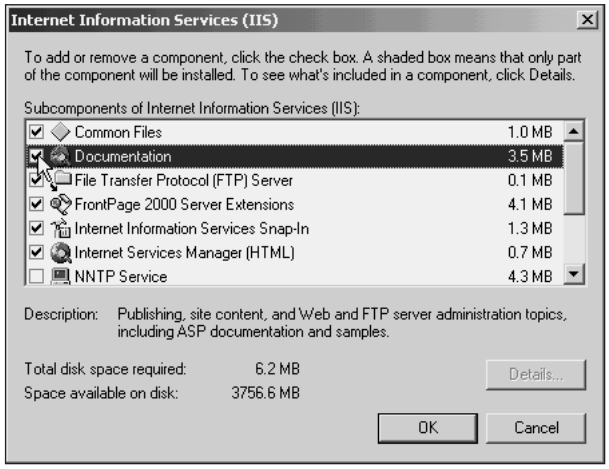

Figure 13-1 Specifying Internet Information Services components

6. Click Next.
7. Insert the Windows 2000 Server CD-ROM, specify the path to the CD-ROM drive and the \I386 folder, and click OK.
8. Click Finish.
9. Close the Add/Remove Programs tool, if it remains open.

Table 13-1 Internet Information Services Components

IIS Component Option	Purpose
Common Files	Files needed for general IIS functions that must be installed, but should not be installed without installing other services
Documentation	Documentation for publishing to and managing Web and FTP sites
File Transfer Protocol (FTP) Server	Used to set up FTP server services for Internet, intranet, and virtual private network (VPN) file transfers between the Windows 2000 server and a client
FrontPage 2000 Server Extensions	Used to work with Microsoft FrontPage and Visual InterDev for creating and publishing Web materials developed through those tools (both tools are purchased separately)
Internet Information Services Snap-In	Installs an MMC snap-in that is used to manage an IIS server
Internet Services Manager (HTML)	Sets up a browser-based tool to manage an IIS server that is in HTML format
NNTP Service	Enables an IIS server to function as a Network News Transfer Protocol server to provide newsgroups and news messages to client subscribers

Table 13-1 Internet Information Services Components (continued)

IIS Component Option	Purpose
SMTP Service	Enables an IIS server to function as a Simple Mail Transfer Protocol server (see Chapter 3) to distribute SMTP-formatted e-mail messages on a network or through the Internet
Visual InterDev RAD Remote Deployment Support	Used to remotely deploy (on another server) applications developed through the Microsoft Visual InterDev Rapid Applications Development (RAD) tool
World Wide Web Server	Enables the IIS server to function as a Web server on the Internet, via an intranet, or through a VPN

When you install IIS, it sets up the services you selected so that they start automatically each time the server is booted. Some services, such as the SMTP service, can be checked using the Computer Management tool. Other services are optimized to run as part of the IIssrv.exe program that runs in the background. You can view this program by using Windows 2000 Task Manager (review Hands-on Project 1-7 in Chapter 1). If you experience problems, use both the Task Manager and the Computer Management tool to check that the IIssrv.exe and IIS services are started.

After IIS is installed, click the Next button in the Windows 2000 Configure Your Server window to further configure IIS. In the next window (see Figure 13-2), you have the option to create a virtual directory in which to store HTML and other documents to publish on the Web site. Two other options in the window are to click *Manage* to start administering the IIS Web server and to click *Learn more* to view IIS documentation. Creating a virtual directory and managing the server are described in the next sections.

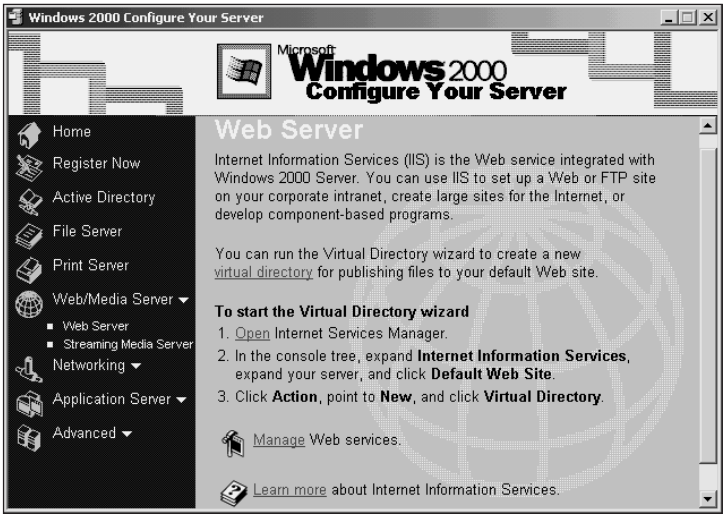

Figure 13-2 Configuring an IIS Web server

Creating a Virtual Directory

A **virtual directory** is really an actual folder on an IIS Web server that is also associated with a **Uniform Resource Locator** (**URL**) so that it can be accessed over the Internet, an intranet, or a VPN. The reason for creating a virtual directory is to provide an easy way for multiple users to publish on the Web site, by modifying and uploading files to the virtual directory. A URL is a special addressing format used to find particular Web locations. When you set up a virtual directory, you give it an alias, which is a name to identify it to a Web browser. The URL format for accessing a file in a virtual directory entails providing the server name, the virtual directory alias, and the filename, for example: \\Lawyer\Webpub\Mypage.html. In this example, Lawyer is the server name, Webpub is the alias of the virtual directory, and Mypage.html is the file.

To create a virtual directory, access the Internet Information Services management tool by clicking the Open hyperlink shown in Figure 13-2 or by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking Internet Services Manager. Double-click the Web server in the tree, right-click Default Web site in the tree, point to New, click Virtual Directory, and use the wizard to create the virtual directory (try Hands-on Project 13-2). When you create a virtual directory, you can choose the security options you want to apply, shown in Table 13-2.

Table 13-2 Virtual Directory Security Options

Security Option	Purpose
Browse	Enables users to browse the contents of the virtual directory
Execute	Enables users to execute programs and scripts
Read	Enables users to open files in the virtual directory
Run scripts	Enables users to run command scripts
Write	Enables users to add new files to the virtual directory and to modify the contents of existing files

After a virtual directory is created, you can modify its properties in the Internet Information Services tool by clicking Default Web Site in the tree under the server, right-clicking the virtual directory's alias, such as WebPub, and then clicking Properties (see Figure 13-3). Table 13-3 presents a general description of the properties that can be configured for a virtual directory.

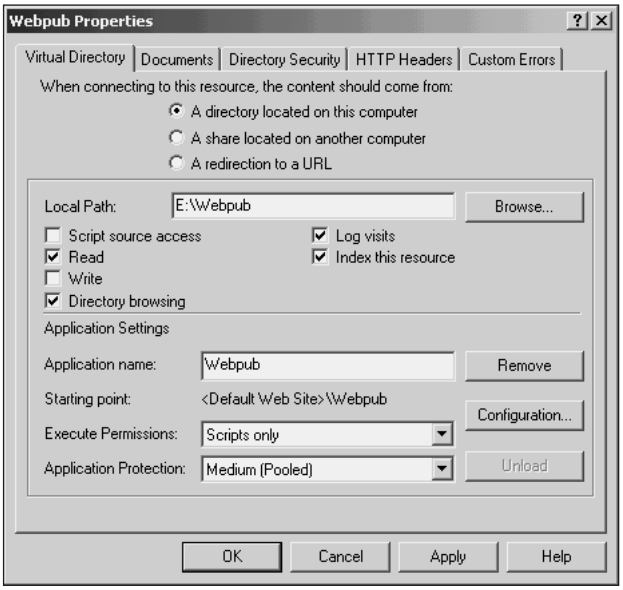

Figure 13-3 A virtual directory's properties

Table 13-3 Virtual Directory Properties Tabs

Properties Tab	Purpose
Virtual Directory	Used to specify general properties that include the computer on which the physical folder is located, the local path, security, and application settings
Documents	Used to define a default Web page and to specify a footer for Web documents
Directory Security	Used to fine-tune security, including whether to allow anonymous access, to set IP address restrictions and restrictions on domain names that can access the site, and to require secure communications through certificates
HTTP Headers	Used to set an expiration date on the directory contents, to set properties of headers that are returned to the client's browser, to set content ratings (such as for content limited to adults), and to specify Multipurpose Internet Mail Extensions (MIME)
Custom Errors	Used to set up error messages that are displayed in a client's browser when specific errors occur

The physical folder properties, including permissions, share permissions, and Web sharing permissions (see Chapter 9), can also be modified by right-clicking the folder and choosing properties in Windows Explorer or My Computer when you are directly logged on to the server.

Managing and Configuring an IIS Web Server

After it is installed, you can manage a Web server using the Internet Information Services tool, also called the Internet Services Manager, described in the previous section. You can access the tool in several ways. One way is to click the *Manage* hyperlink in the Windows 2000 Configure

Your Server window shown in Figure 13-2. Two other ways are to use the Internet Information Services MMC snap-in or to click Start, point to Programs, point to Administrative Tools, and click Internet Services Manager.

The Internet Information Services tool enables you to manage the following types of IIS components (depending on which components you have installed):

- Default Web site
- Administration Web site
- FTP site
- SMTP virtual server
- NNTP virtual server

The Default Web site component is used to manage WWW services offered through an IIS server. The Administration Web site enables you to manage multiple IIS servers from one administrative Web server. FTP site is for managing FTP services offered through an IIS server. The SMTP and NNTP virtual server components are used to manage Internet e-mail and newsgroup services on an IIS server. To manage any of these components, open the Internet Information Services tool and double-click the IIS server in the tree under Internet Information Services (see Figure 13-4). Next, click the component under the tree, for example Default Web Site.

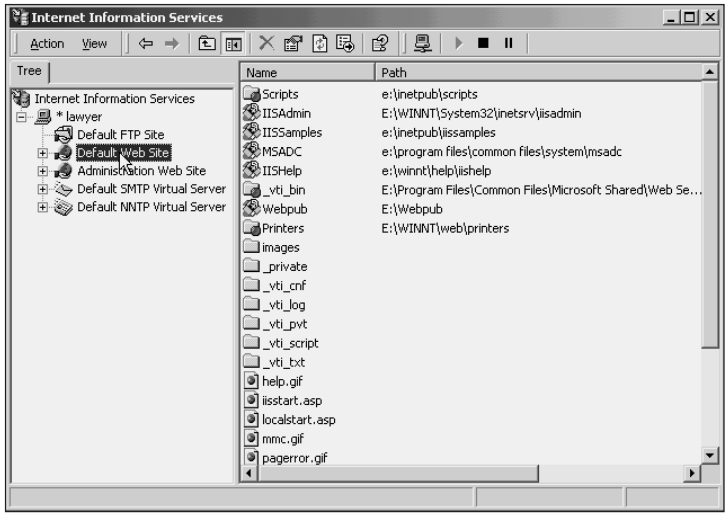

Figure 13-4 Managing a Web site

There are many parameters that you can configure for a Web site, but the best advice is to start by configuring the basic properties, for example configuring performance to match the number of users, and configuring security.

To configure an IIS Web server, open the Internet Information Services tool and double-click Internet Information Services in the tree to display the name of the Web server. Double-click the server in the tree, right-click Default Web Site in the tree (or in the right pane), and click Properties. Click the Web Site tab, if it is not displayed already, and begin configuring properties (see Figure 13-5). For example, make sure that the IP address for the Web site is specified in the IP Address box. You can make one Web site appear as several different sites by clicking the Advanced button and configuring additional IP addresses. Optimize the Web site by clicking the Limited To radio button and setting a limit on the number of connections, to match or exceed the traffic that you anticipate for the server, for example 100 simultaneous connections for a small site or 500 for a medium-sized site.

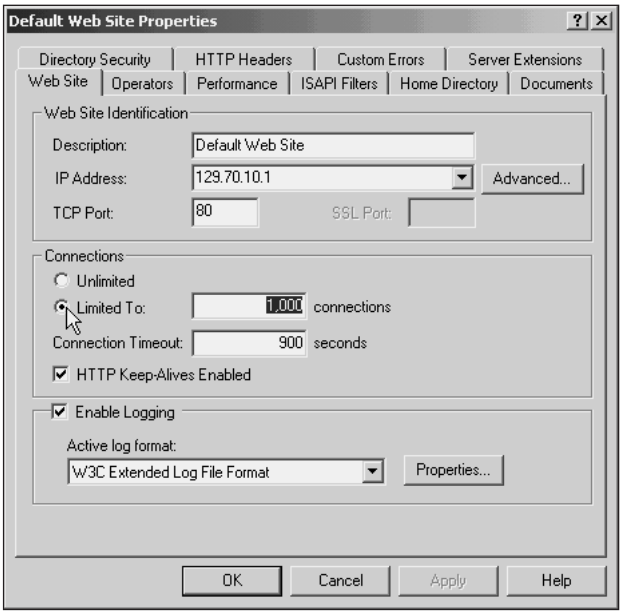

Figure 13-5 Configuring Web site properties

Click the Performance tab and configure the Web site for the number of users (or "hits") who access the site on a given day. The options are: Fewer than 10,000, Fewer than 100,000, and More than 100,000. Next, click the Directory Security tab to establish security. Click the Edit button on the tab to specify if anonymous access is allowed (access in which the user does not have to provide identification). Also, specify the type of authentication, from the following choices:

- *Basic authentication (password is sent in clear text):* Used for clients who cannot send an encrypted password
- *Digest authentication:* Used to transmit a hashed security communication, and not a password, between the Web server and the client. A hashed value is created by using a mathematical formula to create a random value.

- *Integrated Windows authentication:* Uses a secret code prepared by a cryptographic formula between the client and the Web server to authenticate the client, instead of using a password.

Two other options to create secure communications are to set IP restrictions and to secure communications through the use of certificates. The next section discusses how to set up IP restrictions when the Web server is designed to be a VPN server (see Chapter 12).

Table 13-4 presents a summary of the Web site Properties tabs.

Table 13-4 Default Web Site Properties Tabs

Properties Tab	Purpose
Web Site	Used to configure IP addressing, number of connections, connection time-out, and activity logging
Operators	Used to specify which user accounts and groups have privileges to manage the Web server
Performance	Used to optimize performance on the basis of daily hits, bandwidth, and CPU/process utilization
ISAPI Filters	Used to set up Internet Server Application Programming Interface (ISAPI) filters, which are used to provide special instructions on how to handle specific HTTP requests
Home Directory	Specifies the location of the main folder in which Web programs and processes are stored (which is usually \\server\inetpub\wwwroot) and enables you to set security on that folder
Documents	Defines a default Web page for the Web site and enables you to specify a footer for Web documents
Directory Security	Used to set up security for a Web site, including whether to allow anonymous access, authentication methods, IP address and domain restrictions, and use of certificate security
HTTP Headers	Used to set an expiration date on the directory contents, to set properties of headers that are returned to the client's browser, to set content ratings (for example, for content limited to adults), and to specify Multipurpose Internet Mail Extensions (MIME)
Custom Errors	Used to set up error messages that are displayed in a client's browser when specific errors occur while accessing the Web server
Server Extensions	Used to establish security and controls for publishing documents using FrontPage

Configuring IP and Domain Security Access for Intranets/VPNs

You can limit access to a Web server by setting restrictions on which IP addresses, which subnet mask, and which domains can access the server. You would set these restrictions when you create a combined Web and VPN server, for example. In this instance, you can set up the VPN server access to be controlled through the physical WAN or router connection; you can limit access even further by setting up restrictions on which individuals and groups can access

the server through IP address restrictions and by restricting access to only certain domains. For example, consider a VPN server configured for access to Web services in which you want to limit access to only those users on subnets 177.28.19 and 177.28.23. Also, you want to grant 10 other users access on the basis of their unique IP addresses. You can restrict the access to the Web services by opening the Internet Information Services management tool, double-clicking the Web server in the tree, right-clicking Default Web Site, and clicking Properties. Click the Directory Security tab and the Edit button for access by IP addresses. Deny access to all computers, except those in the groups 177.28.19 and 177.28.23 and the 10 single computers that you specify by IP address (see Figure 13-6). Try Hands-on Project 13-3 to practice restricting a Web site for use on a VPN.

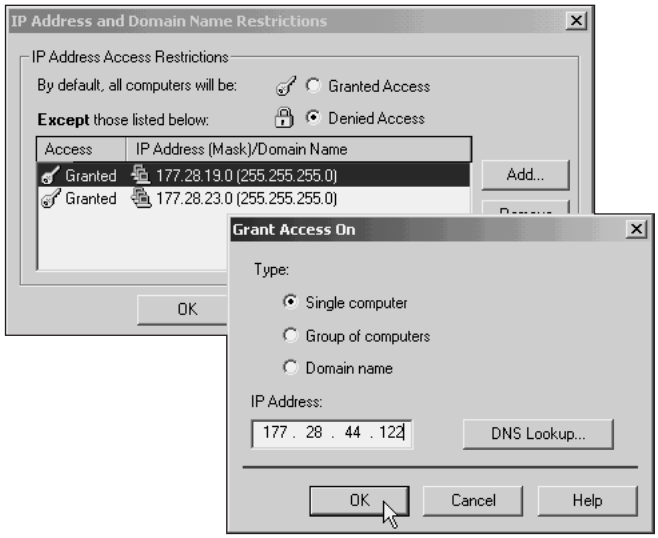

Figure 13-6 Configuring restricted IP access

Troubleshooting a Web Server

Occasionally a Web server used for a Web site, intranet, or VPN can experience problems—for example, users cannot connect to the server, or the server is not enabling e-mail to be sent. Table 13-5 illustrates possible problems and their solutions.

Table 13-5 Troubleshooting IIS

Problem	Solution(s)
The Web server is not responding.	1. Use the Network and Dial-up Connections tool to make sure that the server's connection to the network or Internet is enabled. 2. Use the Task Manager to make sure that the IIssrv.exe program is working. 3. Right-click the Web server in the IIS management tool and click Restart IIS to restart the IIS service. 4. Use the Computer Management tool to make sure that the Server and Workstation services are started and set to start automatically.
No one can access the Web server, but the server is booted and its network and Internet connections are enabled.	1. Make sure there is a WINS server on the network and that it is functioning. 2. Make sure that the DNS server(s) is(are) connected and working on the network. 3. Use a Web browser from different computers and locations to test the connection and determine if the problem is due to a network segment location, the Internet connection, or a specific client that cannot access the server.
Clients can connect to the Web server, but cannot access its contents.	1. Make sure that the authentication and encryption set at the server match the authentication and encryption properties that the client computers can support. 2. Check the Web sharing permissions on Web folders to make sure that they enable the appropriate client access, such as permission to read files and run scripts (try using the IIS Permissions Wizard for help, or check the folders' properties). 3. Make sure that no NTFS permissions on Web folders are set to Deny. 4. Make sure that the \Inetpub\wwwroot folder is intact and contains all of the necessary HTML files (open the IIS management tool, right-click Default Web Site, and click Open).
FTP to the Web server does not work.	1. Make sure that the File Transfer Protocol (FTP) Server service is installed as a Windows component through the Add/Remove Programs tool. 2. Grant the appropriate permissions on folders used for FTP, including the ability to write for those who upload documents to the server. 3. Use the Computer Management tool to make sure that the FTP Publishing Service is started and set to start automatically.

Table 13-5 Troubleshooting IIS (continued)

Problem	Solution(s)
E-mail is not going through the Web server.	1. Make sure that the SMTP service is installed as a Windows component through the Add/Remove Programs tool. 2. Use the Computer Management tool to make sure that the Simple Mail Transfer Protocol service is started and set to start automatically.
Newsgroups are not supported on the Web server.	1. Make sure that the NNTP service is installed as a Windows component through the Add/Remove Programs tool. 2. Make sure that there are virtual directories set up for newsgroups and that the permissions are appropriately set for users to access, for example permissions to browse and read. 3. Use the Current Sessions tool in the IIS management tool to determine if users are connecting to the service.
Users cannot publish using FrontPage.	1. Make sure that the FrontPage 2000 Server Extensions are installed as a Windows component through the Add/Remove Programs tool. 2. Encourage users to upgrade to FrontPage 2000 for best compatibility.

Installing Windows Media Services

When multimedia applications are played in **streaming** mode, the audio and video begin playing as soon as received, without waiting for the entire file to be received at the client. A Windows 2000 Server can be set up to provide streaming media services by installing the Windows Media Services component. The Windows Media Services component is separate from the Internet Information Services component and can be installed after you install IIS. Media services enable you to serve voice and video multimedia applications from a Web server—for example, an audio/video lesson demonstrating a hazardous chemistry experiment that is too dangerous for students to try in a lab on their own. When you install Microsoft Windows Media Services, you must also install the Windows Media Services Administrator, which is used to manage the services. Hands-on Project 13-4 enables you to practice using the Add/Remove Programs tool in the Control Panel to install the media services and administrator.

To use the media services, determine if your applications are capable of unicasting or multicasting, as described in Chapter 3 (multicasting is more efficient). You can configure the server for either type of transmission by using the Windows Media Services Administrator. Open the Windows Media Services Administrator from the Administrative Tools menu (try Hands-on Project 13-4), and click Configure Server for instructions about how to configure the server for a specific type of application (see Figure 13-7).

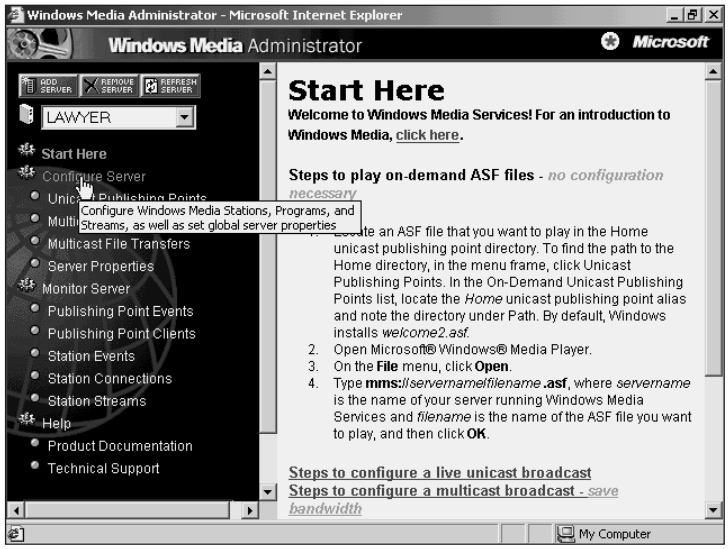

Figure 13-7 Windows Media Services Administrator

INSTALLING MICROSOFT DNS SERVER

One of the requirements for running IIS is to have a domain name resolution service available to it, such as Domain Name Service (DNS) or Windows Internet Naming Service (WINS) (see Chapters 3 and 4). If there is not a DNS server on your network, you will need to install Microsoft DNS Server, WINS, or both. **DNS Server** is a Microsoft service that resolves IP addresses to computer names, such as resolving 129.77.1.10 to the computer name Brown; it also resolves computer names to IP addresses. WINS is used with DNS Server to resolve IP addresses and computer names on networks in which NetBIOS applications are still in use, including NetBIOS computer names for pre-Windows 2000 clients, such as Windows 95, 98, and NT (see Chapter 3).

When you implement the Active Directory, it also requires at least one DNS server and will prompt you to automatically install the Microsoft DNS service, if a DNS server is not already present on the network. If you use the Active Directory and have two or more domain controllers (DCs), plan to set up Microsoft DNS services on at least two of the DCs, because the multimaster replication model (see Chapter 4) enables you to replicate DNS information on each DC. The advantage of replicating DNS information is that if one DC that hosts DNS services fails, another DC is available to provide uninterrupted DNS services for the network. This is especially critical on a network that provides Internet access and Web-based SMTP e-mail services.

Microsoft DNS Server is installed from the Control Panel Add/Remove Programs icon, using the following steps:

1. Click Start, point to Settings, and click Control Panel.
2. Double-click Add/Remove Programs.
3. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
4. Double-click Networking Services to view the individual components that can be installed and to check Domain Name System (DNS), as in Figure 13-8. Click OK in the Networking Services dialog box.

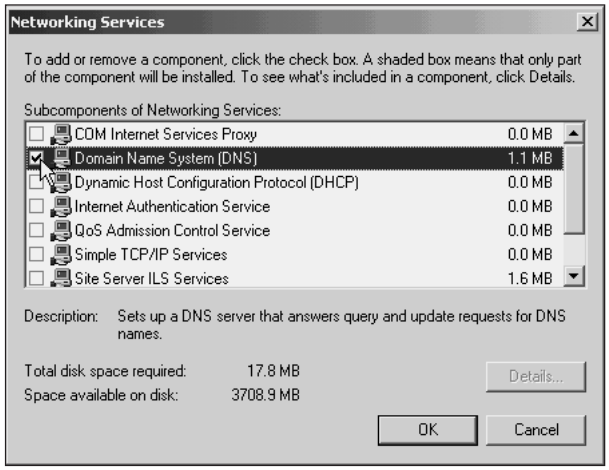

Figure 13-8 Installing Microsoft DNS

5. Click Next in the Windows Components Wizard dialog box.
6. If requested, insert the Windows 2000 Server CD-ROM, specify the path to the CD-ROM drive and the \I386 folder, and click OK.
7. Click Finish.

Microsoft recommends that DNS servers have a static IP address (one that is manually configured, not automatically assigned by DHCP; see Chapters 3 and 6). Also, before installing DNS on a server when the Active Directory is in use on a network, make sure that the server is a DC, or promote it to be a DC if it is not. Use the Dcpromo tool to promote a member server to a DC by clicking Start, clicking Run, entering *dcpromo*, and clicking OK. When you use Dcpromo, the program will inform you whether the computer is a DC. *If the computer is already a DC, click Cancel when the Active Directory Installation Wizard starts, because if you continue, the wizard will remove the Active Directory setup on that computer*.

After you install DNS Server, it is necessary to configure it through the DNS management tool, which can be accessed from the DNS MMC snap-in or by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking DNS. Use the DNS Manager to create two primary zones of DNS information. One zone, called the **forward lookup zone**, holds host name records, called address records, to map a computer name to the IP address. Each IP-based server and client should have a host record so that it can be found through DNS. For example, if the DNS server name is Lawyer, with the IP address 129.70.10.1, then the forward lookup zone maps Lawyer to 129.70.10.1. In IP version 4, a host record is called a **host address (A) resource record**. Figure 13-9 shows the forward lookup zone host records as shown in the DNS management tool. When you install DNS on a DC in a domain, a forward lookup zone is automatically created for the domain, with the DNS server record already entered. You must enter the records of other hosts or configure DHCP to automatically update the DNS forward lookup zone each time it assigns an IP address.

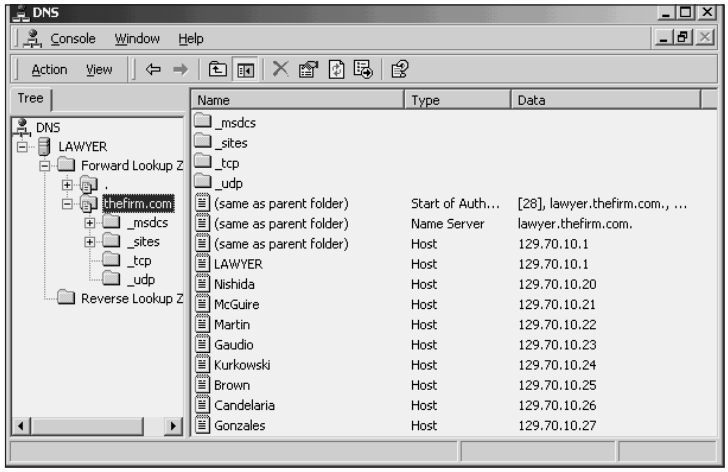

Figure 13-9 DNS forward lookup zone

At this writing, IP version 4 is a 32-bit address (4 octets) and is used in most places. IP version 6 (IPv6) is under development and consists of a 128-bit address. An IPv6 record is called an IPv6 host address (AAAA) resource record. Windows 2000 Server DNS is compatible with both types of host records.

Depending on the domain structure and Internet connectivity, a DNS server can have several forward lookup zones, but there should be at least one for the parent domain, such as *thefirm.com*. On the Internet, this is called a second-level domain name because it is constructed from "thefirm" and "com." The first level is the root, which indicates the type of Internet site, such as "com," which denotes that this is a company and not an educational institution (edu), for example.

Another zone, called the **reverse lookup zone**, holds the **pointer (PTR) resource record**, which contains the IP-address-to-host name. The reverse lookup zone is not as commonly used as the forward lookup zone, but can be important to create for those instances

when a network communication requires associating an IP address to a computer name, such as for monitoring a network using IP address information. Because it is used less commonly, the reverse lookup zone is not automatically created when DNS is installed. To create the reverse lookup zone:

1. Open the DNS management tool, and double-click the DNS server in the tree, if the child objects under it are not displayed.
2. Click Reverse Lookup Zone to select it, click the Action menu, and click New Zone.
3. Click Next after the New Zone Wizard starts.
4. If the Active Directory is installed, click *Active Directory Integrated* for the type of zone to create. This option integrates storage of DNS information with the Active Directory and enables you to replicate DNS information among DCs. If the Active Directory is not installed (or if you do not want to integrate DNS data with the Active Directory—which is not recommended), click Standard primary, which puts the data into a text file. Click Next.
5. Enter the network ID of the reverse lookup zone (which is the first two or three octets that identify the network, depending on the subnet mask that you use). This information is used to build the "in-addr.arpa" reverse lookup zone name. For example, if your zone network address is 129.70, then the in-addr-arpa reverse lookup zone is named 70.129.in-addr.arpa. The Wizard automatically builds the in-addr-arpa name format when you enter the network address (see Figure 13-10). Click Next. If the wizard asks whether to create a new file or use an existing file, select to create a new file and then click Next.

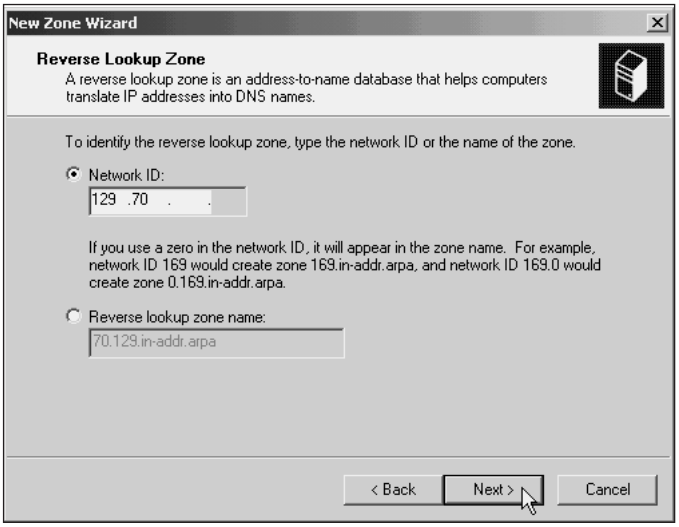

Figure 13-10 Creating a reverse lookup zone

6. Review the information you have entered, and click Finish.
7. If you are using subnets, you can create a folder for each one under the parent reverse lookup zone by right-clicking the new zone, such as 129.70.x.x Subnet, clicking New Domain, and entering the subnet value, such as 10 (for subnet 129.77.10). Click OK, and repeat this step for each subnet. Figure 13-11 illustrates the way the new subfolder is displayed in the DNS management tool.

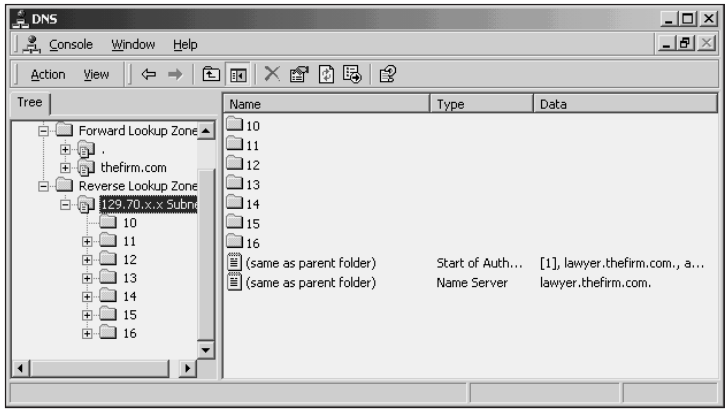

Figure 13-11 Reverse lookup zone subfolders for subnets

After the two primary zones are created, it is necessary to populate each zone with records, to enable forward and reverse address translations. If DHCP is set up to work with DNS, it will automatically populate the zones. You also have the option of manually entering records for servers and clients. For example, to enter a forward lookup zone host address (A) resource record using the DNS management tool, double-click the DNS computer and Forward Lookup Zones in the tree. Right-click the domain name, click New Host, enter the host name and IP address, and check *Create associated pointer (PTR) record* to automatically create the reverse zone record (see Figure 13-12). To manually create a reverse lookup zone record in the tree under the DNS server, double-click Reverse Lookup Zones and double-click to display the appropriate subfolder for the computer's subnet. Right-click the subfolder representing the subnet, click New Pointer, and enter the IP address and host name (see Figure 13-13). Try Hands-on Project 13-5 to practice creating forward and reverse lookup zone records.

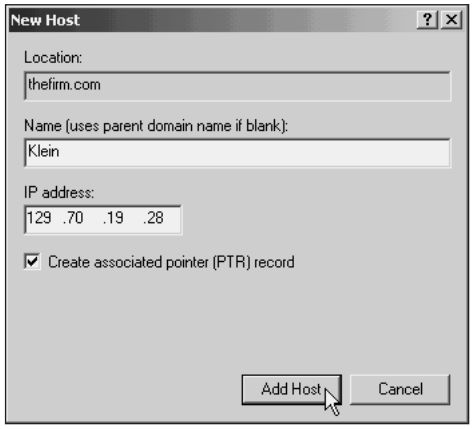

Figure 13-12 Creating a host address (A) resource record

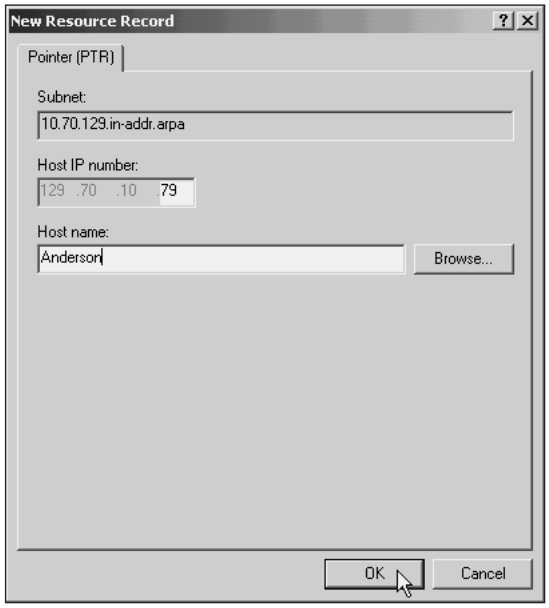

Figure 13-13 Creating a PTR record

The forward lookup zone is used more frequently than the reverse lookup zone, because network hosts (servers and clients) are most commonly identified by their computer names. For instance, when you want to access a shared folder or a Web server, you usually do so by using the computer's name or the Web server's domain identification, not the IP address. For another example, when you access Microsoft's Web site at *microsoft.com*, the DNS servers at that site use the forward lookup zone to link the domain name with the appropriate Web server by IP address.

If DNS is installed, but is not resolving names, or does not seem to be working, check to make sure that the DNS Server and DNS Client services are both started and set to start automatically on the DNS server.

To check that the DNS Server and DNS Client Services are started, click Start, point to Programs, point to Administrative Tools, and click Computer Management (or right-click My Computer and click Manage). Double-click Services and Applications in the console tree, and click Services. Scroll to view the DNS Client and DNS Server services, and then check the status and startup type information for both. If you need to start one or both services, double-click the service and click the Start button. Also, make sure that the Startup type box is set to Automatic. The DNS Server service is dependent on the NT LM Security Support Provider and the Remote Procedure Call (RPC) services, so make sure both of these services also are started and set to start automatically.

Installing Microsoft WINS

WINS is used to register NetBIOS computer names and map them to IP addresses for pre-Windows 2000 servers and clients. WINS automatically registers network clients that use NetBIOS and builds a database that other network clients can query in order to locate a computer. For example, if there is a Windows 95 network computer called Eggplant that offers a shared folder for other network clients, those other clients can query WINS to find Eggplant. WINS also makes it possible for NetBIOS-named computers to send and receive SMTP e-mail over the Internet.

The steps for installing WINS are nearly the same as for installing DNS, using the Add/Remove Programs tool in the Control Panel. The difference is that when you select which network service to install, you choose Windows Internet Name Service (WINS), as follows:

1. Open Add/Remove Programs in the Control Panel.
2. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
3. Double-click Networking Services, and check Windows Internet Name Service (WINS). Click OK in the Networking Services dialog box.
4. Click Next in the Windows Components Wizard dialog box.
5. If requested, insert the Windows 2000 Server CD-ROM, specify the path to the CD-ROM drive and the \I386 folder, and click OK.
6. Click Finish.

Plan to use the default configuration for WINS after it is installed. If you need to manage WINS, you can access the WINS management tool as an MMC snap-in or from the Administrative Tools menu. For example, you can use this tool to import a special database of computers to register, or to set up replication with other WINS servers in a domain.

INSTALLING MICROSOFT DHCP

The Dynamic Host Configuration Protocol (DHCP, see Chapter 3) is a protocol in the TCP/IP suite that is used along with DHCP services to detect the presence of a new network client and assign an IP address to that client. When you set up a Windows 95, 98, NT, or 2000 client to automatically obtain an IP address, the client contacts a DHCP server to obtain an address. The DHCP server has a preassigned range of IP addresses that it can give to new clients. Each address is assigned for a specific period of time, such as eight hours, two weeks, a month, or a year. A range of contiguous addresses is called the **scope**. A single Microsoft DHCP server can support the following:

- Dynamic configuration of DNS server forward and reverse lookup zone records
- Up to 1000 different scopes
- Up to 10,000 DHCP clients

A Windows 2000 server can be configured as a DHCP server using Microsoft DHCP services. When you set up a Microsoft DHCP server, you have the option of setting it up to automatically enter forward and reverse lookup zone records in a Microsoft DNS server. The DHCP server automatically updates the DNS server at the time it assigns an IP address. Using dynamic DNS updates can significantly save time in creating DNS lookup zone records.

Multiple scopes are supported in a single Microsoft DHCP server, because it is often necessary to assign different address ranges, such as one range that is 129.70.10.1 to 129.70.10.122 and another that is 129.70.20.10 to 129.70.20.78. As this example illustrates, you can assign address ranges to reflect the network subnet structure or other network divisions.

If your network has Internet connectivity, make sure you obtain IP address ranges from your Internet service provider, so that you use addresses that are specifically assigned to your organization and recognized as valid by the Internet community.

DHCP is installed using the Control Panel Add/Remove Programs tool as a networking service in the Windows components. To install DHCP:

1. Open Add/Remove Programs in the Control Panel.
2. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
3. Double-click Networking Services, and check Dynamic Host Configuration Protocol (DHCP). Click OK in the Networking Services dialog box.
4. Click Next in the Windows Components Wizard dialog box.
5. If requested, insert the Windows 2000 Server CD-ROM, specify the path to the CD-ROM drive and the \I386 folder, and click OK.
6. Click Finish.

Configuring a DHCP Server

After DHCP is installed, it is necessary to set up one or more scopes and to authorize the DHCP server. The process of authorizing the server is a security precaution to make sure that IP addresses are only assigned by DHCP servers that are managed by network and server administrators. The security is needed because it is critical that IP address assignment be carefully managed to ensure that only valid IP addresses are used and that there is no possibility that duplicate IP addresses can be assigned. DHCP servers that are not authorized are prevented from running on a network. A third step that is not required, but that saves time in managing DNS, is to configure the DHCP server and its clients to automatically update DNS records.

Only DCs and member servers can be authorized as DHCP servers when the Active Directory is in use on the network. If the Active Directory is not implemented, a standalone server can be authorized.

Managing a DHCP server is accomplished through the DHCP management tool, which is accessed as an MMC snap-in or by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking DHCP. To start the New Scope Wizard, open the DHCP management tool, double-click DHCP, right-click the DHCP server, click New Scope, and complete the steps presented by the wizard (try Hands-on Project 13-6). Figure 13-14 illustrates how to enter an address range via the wizard.

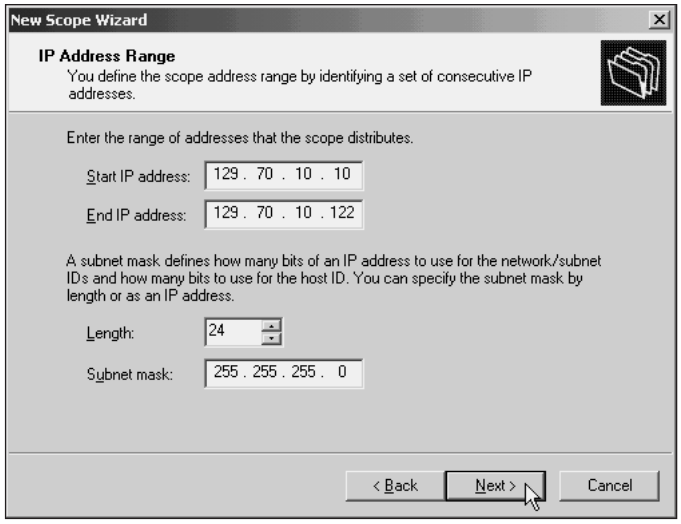

Figure 13-14 Creating a scope

Set the duration of a lease on the basis of the type of connection. For desktop computers that are connected on a more permanent basis, set leases to expire after a longer period, such as from three days to a couple of weeks. Particularly, use a longer lease period on medium-and large-sized networks in which you have a large number of IP addresses that can be used. For laptop and portable computers that are less permanent on the network, set leases to expire after the duration of the communication session, such as 8–24 hours.

To authorize a DHCP server in the Active Directory via the DHCP management tool after you create a scope (you must be logged on as Administrator or as an Enterprise Administrator):

1. Right-click the server as you did when creating the scope.
2. Click Authorize on the menu.

When it is installed, a DHCP server is automatically configured to register IP addresses at the DNS servers, but you must also provide the DNS servers' IP addresses when you configure each scope. You can make sure that automatic DNS registration is set up on the DHCP server by right-clicking the server in the DHCP management tool and then clicking Properties. Click the DNS tab to check its setup (see Figure 13-15). The *Automatically update DHCP client information in DNS* box should be checked. If all clients are running Windows 2000 operating systems, and you want the clients to update the DNS server records, check the radio button to *Update DNS only if DHCP client requests*. Windows 2000 clients can automatically communicate with the DNS server to perform their own updates. If some clients are running Windows 95, 98, or NT, then click the radio button to *Always update DNS*, which means that the DHCP server takes the responsibility to update the DNS server's records every time a client obtains the IP address. Also, make sure that *Discard forward (name-to-address) lookups when lease expires* is checked, so that the DHCP server alerts the DNS server to delete a record each time a lease is up. If some clients are running Windows 95, 98, or NT, also check *Enable updates for DNS clients that do not support dynamic update*.

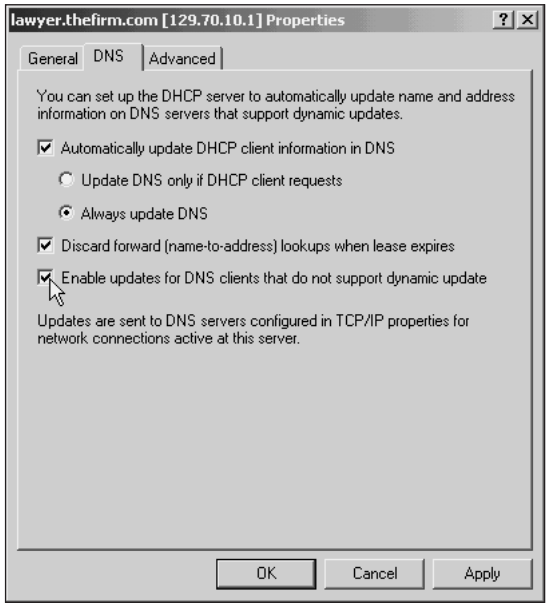

Figure 13-15 Configuring automatic DNS registration

Troubleshooting DHCP

When you set up a DHCP server, it is possible for problems to occur. Some possible problems include, among others: (1) the server is stopped or not working, (2) it is creating extra network traffic, and (3) it is not automatically registering with DNS servers. Table 13-6 presents several typical problems and their resolutions.

Table 13-6 Troubleshooting a DHCP Server

Problem	Solution(s)
The DHCP server will not start.	1. Use the Computer Management tool to make sure that the DHCP Client and DHCP Server services are started and set to start automatically. If the DHCP Server service will not start, make sure that the Remote Procedure Call (RPC) and the Security Accounts Manager services are already started, because the DHCP Server service depends on both. 2. Make sure that the DHCP server is authorized.

Table 13-6 Troubleshooting a DHCP Server (continued)

Problem	Solution(s)
The DHCP server creates extra or excessive network traffic.	Increase the lease period in each scope, so there is less traffic caused by allocating new leases when the old ones expire.
The DNS lookup zone records are not automatically updated.	1. Make sure that DNS servers and IP addresses are set up in each DHCP scope. 2. Make sure that the DHCP server's properties are set up to automatically update the DNS server. Also, have the DHCP server do the updating, instead of clients, when there are pre-Windows 2000 server clients. Last, enable DNS updating for clients that do not dynamically support it.
One of the leased IP addresses is conflicting with a permanent IP address assigned to a computer, such as a server.	Exclude that IP address from the scope.
Your network has a large number of portable and laptop computers and is in short supply of IP addresses.	Reduce the lease duration so that leases expire sooner and can be reassigned.
The System log is reporting Jet database error messages.	The DHCP database is corrupted. Have users log off from the DHCP server, and disable the server's connection (use the Network and Dial-up Connections tool). Use the DHCP management tool to reconcile the scopes (right-click the server and click Reconcile All Scopes). Another option is to open the Command Prompt window and use the Jetpack.exe program to repair the database. A third option is to use the Nesh.exe command to dump the database and then reinitialize it.
The DHCP server is not responding.	Use the Network and Dial-up Connections tool to make sure that the server is connected to the network.

Connecting Through Terminal Services

Besides using Windows 2000 as a Web, DNS, or DHCP server, you can also use it as a terminal server. A **terminal server** enables clients to run services and software applications on the Windows 2000 server instead of at the client, which means that nearly any type of operating system can access Windows 2000. The Windows 2000 Terminal Services are used for three broad purposes: to support thin clients, to centralize program access, and to remotely administer Windows 2000 servers. One of the main reasons for using a terminal server is to enable **thin clients**—such as specialized PCs that have minimal Windows-based operating systems—to access a Windows 2000 server, so that most CPU-intense operations (creating a spreadsheet for example) are performed on the server. Some examples of thin client computers are Hewlett-Packard's Netstation, Maxspeed's MaxTerm, Neoware's NeoStation, and Wyse Technologies'

Winterm terminals. These function similarly to a basic **terminal** that has no CPU and that accesses a mainframe computer to perform all program execution and processing on the mainframe. Thin client network implementations are generally used to save money and reduce training and support requirements. Also, they are used for portable field or handheld remote devices, such as remote hotel reservation terminals and inventory counting devices. Thin client computers typically cost hundreds of dollars less than full-featured PCs, and because the operating system is simpler it is easier to train users. Thin client field devices can be made inexpensively and tailored for a particular use, such as taking inventory in warehouses.

The second reason for using a terminal server is to centralize control of the way programs are used. Some organizations need to maintain tight control over certain program applications, such as sensitive financial applications, top-secret program development, word-processed documents, and spreadsheets. For example, a network equipment company that invents a switch that is 100 times faster than any other on the market can use a terminal server to closely guard access to design documents and programs. These are stored and modified only on the server, which can be configured to provide a high level of security.

If you plan to set up a terminal server for clients to run programs in multiple sessions, consider the CPU and RAM needs in advance. Use a server that has a fast CPU, such as a Pentium III or faster. Also, populate the server with ample RAM (see Chapter 2 for server selection).

The third reason for using a terminal server is to allow a server administrator to remotely access management tools, such as Active Directory Users and Computers, the Computer Management tool, the DNS tool, and others that appear in the Administrative Tools menu or as MMC snap-ins. Remote access enables a server administrator to manage one or more servers from her or his workstation on the same network, or to dial in from home or while traveling.

Windows 2000 Terminal Services support not only thin clients, but other types of client operating systems, including MS-DOS, Windows 3.x, Windows 95, Windows 98, Windows NT, Windows 2000, UNIX, UNIX-based X-terminals, and Macintosh. There are four main components that enable terminal server connectivity, which are shown in Table 13-7.

Table 13-7 Terminal Services Components

Component	Description
Windows 2000 multi-user terminal services	These services enable multiple users to simultaneously access and run standard Windows-based applications on a Windows 2000 server.
Terminal Server Client	This client software runs on Windows 3.11, Windows 95, Windows 98, Windows NT 3.51, Windows NT 4.0, and Windows 2000 to enable the client to run the Windows graphical user interface, which looks like a regular 32-bit version of Windows.

Table 13-7 Terminal Services Components (continued)

Component	Description
Remote Display Protocol (RDP)	This protocol is used for specialized network communications between the client and the server running terminal services. RDP follows the International Telecommunications Union (ITU) T.120 standard to enable multiple communications channels over a single line.
Terminal services administration tools	These tools are used to manage terminal services.

Before you implement terminal services on a Windows 2000 server, determine in advance if you want that server to be able to cache files at the client for offline access, because offline access is not compatible with terminal services and must be turned off.

Installing Terminal Services

Before you install terminal services, determine if you want the server to function as an application server to clients or as a remote administration server for server administrators, because the installation cannot be set up for both on a single server. When you install the terminal services, you have the option of configuring the server as an application server or a remote administration server at the time it is installed. The only way to change the configuration to the other mode is to reinstall the terminal services. Also, if you plan to set up an application server, then one Windows 2000 server must also be configured as a terminal services licensing server.

Windows 2000 terminal services are installed using the Add/Remove Programs tool in the Control Panel. To install terminal services:

1. Open Add/Remove Programs in the Control Panel.
2. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
3. Check the box in front of Terminal Services and make sure that the box is not gray, since a gray box means that not all components are installed. If the box is gray, double-click Terminal Services, check all of the subcomponents, and click OK in the Terminal Services dialog box.
4. If this is the first or only Windows 2000 server configured as a terminal server, also click Terminal Services Licensing in order to license clients to use terminal services.
5. Click Next in the Windows Components Wizard dialog box.
6. Select whether this server is to be a remote administration server for server administrators or an application server (see Figure 13-16). Click Next.

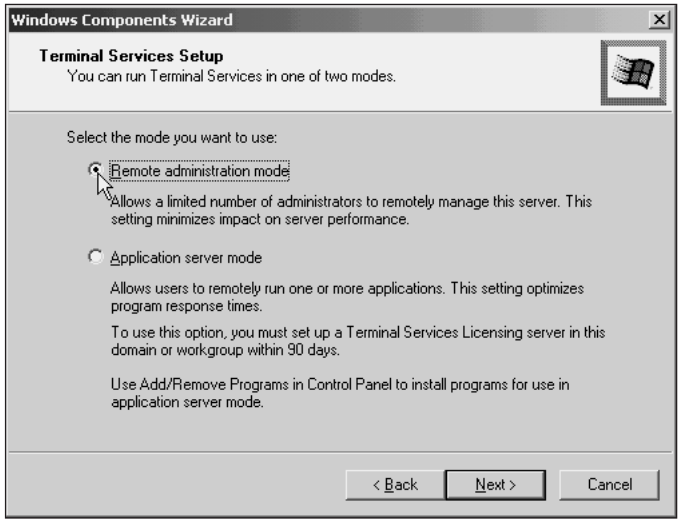

Figure 13-16 Selecting the function of a terminal server

7. If in Step 6 you selected to configure for the application server mode, two dialog boxes are displayed next. The first enables you to specify the security level for access to software applications. You can either use permissions that are compatible with Windows 2000 security or permissions that are less secure for compatibility with some older software applications. The second dialog box shows applications that are currently installed, such as Microsoft Office, and that may need to be reinstalled to function using Terminal Services.
8. If in Step 4 you selected to install Terminal Services Licensing, in the next dialog box click *Your entire enterprise*, if this server is to be used to manage licenses for all clients in an enterprise; click *Your domain or workgroup*, if this server is to be used to manage licensing only for clients in a domain or on a standalone server. Also, select the folder location for the license database. Click Next.
9. If requested, insert the Windows 2000 Server CD-ROM, specify the path to the CD-ROM drive and the \I386 folder, and click OK.
10. Click Finish.
11. Select the option to restart the server to enable the new services to go into effect.

Managing Terminal Services

After the terminal services are installed, three management tools are available in Windows 2000 Server: Terminal Services Client Administrator, Terminal Services Configuration, and Terminal Services Manager. When you install the Terminal Services Licensing component, a fourth tool also is available, Terminal Services Licensing. Table 13-8 lists these tools, including a description of their functions and how to access them.

Table 13-8 Terminal Services Management Tools

Management Tool	Function	Tool Location
Terminal Services Client Creator	Used to make floppy installation disks for clients	Administrative Tools menu
Terminal Services Configuration	Used to configure terminal server settings and connections	Administrative Tools menu and an MMC snap-in
Terminal Services Licensing	Used to administer client licenses for terminal servers in an enterprise or in a single domain	Administrative Tools menu
Terminal Services Manager	Used to control and monitor clients that are connected to terminal services on one or more servers	Administrative Tools menu

Configuring Terminal Services

Begin by using the Terminal Services Configuration tool to configure the remote connection properties. Only one connection is configured for each NIC in the server, which is used to handle multiple clients. For example, click Start, point to Programs, point to Administrative Tools, and click Terminal Services Configuration. Double-click Terminal Services Configuration, if necessary, to view the Connections and Server Settings folders in the tree. Click Connections to view the connection set up during installation. If you have more than one NIC, you can create another connection by right-clicking Connections and clicking Create New Connection. To manage the properties of a connection, double-click the connection in the right pane, such as RDP-Tcp. Figure 13-17 shows the connection Properties dialog box and Table 13-9 describes the capabilities of each tab.

One property that should be checked from the start is permission security (try Hands-on Project 13-7). If the terminal server is used by server administrators for remote administration, make sure that access is set up only for the appropriate administrators group, such as Administrators or Domain Admins. If the terminal server is configured as an application server, first use the Active Directory Users and Computers tool or the Local Users and Groups tool (on a standalone server) to create one or more groups of users who will have access to the terminal server. Then use the Terminal Services Configuration tool to set up the permissions.

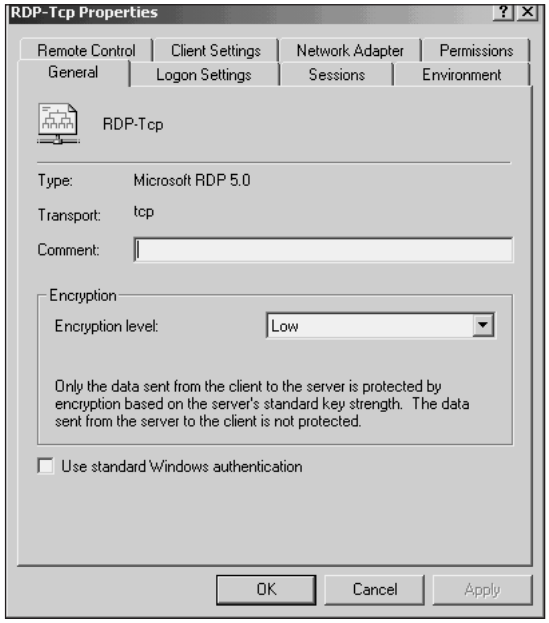

Figure 13-17 Terminal service connection properties

Table 13-9 Terminal Services Components

Tab	Description
General	Used to set up encryption and authentication
Logon Settings	Used to determine how the client logs on, by using information provided by the client or by using a preset logon account setup
Sessions	Used to establish timeout settings and the way clients can reconnect to the server if a session is interrupted
Environment	Enables you to establish a program that runs automatically when the client logs on, and to enable or disable client wallpaper for faster server response
Remote Control	Enables you to remotely control a client or to observe a client's session while that session is active, for example to watch the user's key and mouse strokes to help diagnose a problem without having to go to the client's site
Client Settings	Enables you to configure client connection settings such as whether to use client settings, connect to client drives, or connect to a default printer; also mapping features can be enabled or disabled, such as printer and printer port mapping, clipboard mapping, drive mapping, and audio mapping
Network Adapter	Enables you to specify a NIC to use and to control the number of simultaneous connections
Permissions	Used to set up access permissions by user and by group

Click the Permissions tab to view the defaults that are configured. The Allow and Deny permissions include:

- *Full Control:* Enables access that includes query, set information, reset server, remote control, logon, logoff, message, connect, disconnect, and virtual channel use
- *User Access:* Enables access to query, connect, and send messages
- *Guest Access:* Enables access to logon

Another property that should be checked is the implementation of encryption and authentication. Click the General tab to check these properties. Authentication can be set to use either no authentication or standard Windows authentication when the clients are Windows 95, 98, NT, or 2000. The encryption options are:

- *Low:* Data sent from the client to the server is encrypted.
- *Medium:* Data sent from the client to the server and from the server to the client are encrypted using the default server encryption.
- *High:* Data sent from the client to the server and from the server to the client are encrypted using the highest encryption level at the server.

Configuring a Terminal Services Client

You can configure a client to access a terminal server by making an installation disk using the Terminal Services Client Creator tool, which is started from the Administrative Tools menu. Before you start, format four floppy disks for Windows 3.11, or two disks for Windows 95 or higher and for UNIX systems. Once you start the Terminal Services Client Creator tool, the Create Installation Disk dialog box is displayed (see Figure 13-18). Select the option that fits the client, such as *Terminal Services for 32-bit x86 windows* if the client is running Windows 98. Insert the first disk, and click OK to begin making the disk set. Click OK again to confirm that you want to start making the disks (Hands-on Project 13-7 enables you to practice making installation disks).

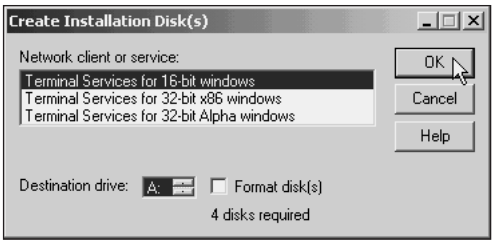

Figure 13-18 Creating a terminal services installation disk

To install the terminal server client software on the floppy disks, for instance on a computer running Windows 95 or Windows 98, insert the first disk in the computer. Click Start, click Run, and enter *a:\setup* in the Open box. Click OK to start the Setup program, which installs the software and creates a program group of the programs used to access the terminal server.

Configuring Licensing

When you set up a terminal server as an application server, you must activate the server and configure licensing by using the Terminal Services Licensing tool (make sure the Terminal Services Licensing component is installed at the same time that you install the Terminal Services component). To open the tool, click Start, point to Programs, point to Administrative Tools, and click Terminal Services Licensing. Double-click *All servers* in the tree to display the servers that offer terminal services. To activate a server, right-click the server in the tree and click *Activate Server*. When the Licensing Wizard starts, click Next and complete the instructions for contacting Microsoft to activate the licenses. There are four ways to contact Microsoft: Internet, World Wide Web, Fax, and Telephone.

If the Terminal Services Manager fails to start properly for a terminal server that is configured as an application server, or if users are unable to connect to the server, check to make sure that you have activated the server using the Terminal Services Licensing tool.

Installing Applications

When you configure a terminal server to function in the applications server mode, applications are installed to be compatible with this mode. For this reason, you may need to reinstall some applications, as noted by the Windows Components Wizard when you install Terminal Services. Use the Control Panel Add/Remove Programs tool to install new applications after the Terminal Services are installed, and use the same tool to uninstall and reinstall programs that were installed prior to setting up the server for Terminal Services.

On a terminal server, software applications are installed only via the install mode, which is automatically invoked when you install applications by clicking Add/Remove Programs in the Control Panel, clicking the Add New Programs button, and clicking the CD or Floppy button to start the program installation. You should not install programs by using the Start menu and Run Option or by double-clicking the installation program from Windows Explorer or My Computer.

Running Windows 16-bit programs, which is accomplished through the virtual DOS machine and Windows on Windows (WOW, see Chapter 1), is not recommended when Windows 2000 Server is set up as a terminal server for applications. When users run 16-bit programs, the CPU can support only 60% of the total number of simultaneous connections that can be supported when only 32-bit programs are run. Also, the amount of RAM used per each 16-bit program is 50% more. MS-DOS programs should not be run at all, because of their high use of CPU resources.

Monitoring Terminal Services

Open the Terminal Services Manager to monitor live sessions and processes. By using the Terminal Services Manager you can:

- View status information about a session
- Connect to view a session or disconnect from one
- Log off a user's session
- Reset a user's session
- Send a message
- End a process
- Control a session remotely

To use any of these features on a user's session, click Start, point to Programs, point to Administrative Tools, and click Terminal Services Manager. Click the name of the server in the console tree. The right-hand pane displays three tabs: Users, Sessions, and Processes. The Users tab identifies user accounts that are connected and shows the sessions they have in progress. The Sessions tab lists sessions first and then the users who are engaged in those sessions. The Processes tab shows the processes currently in use in Windows 2000 Server.

To perform any function on a user's connection, click the Users tab and right-click the connection. The shortcut menu displays the following options: Connect, Disconnect, Send Message, Remote Control, Reset, and Status. For example, to view the status of a connection, right-click that connection and click Status. If you want to watch a user's session while that user is in action, right-click the user and click Connect. When you are finished watching the session, right-click the user again and click Disconnect. Or, if you want to take over the session (for example, to show the user how to do a particular task), right-click the user and click Remote Control.

In Chapter 14, you learn how to use the System Monitor to monitor terminal services.

Troubleshooting Terminal Services

Sometimes users experience problems while using terminal services, such as connecting to the terminal server or logging off because their session is hung. Table 13-10 presents troubleshooting ideas for terminal servers and clients.

Table 13-10 Troubleshooting a Terminal Server

Problem	Solution(s)
The client cannot log on.	1. Make sure that the encryption and authentication set at the server match what the client is capable of handling. 2. Have the client user manually enter her or his username and password instead of relying on the automatic connection. 3. For network connections, make sure that the client is configured to use the same protocol as the server, such as TCP/IP. For dial-up connections, make sure that the client's dial-up connection is using PPP and the same protocol as the server, such as TCP/IP.
The terminal server is not configured to run applications.	Use the Add/Remove Programs tool to uninstall terminal services, and then reinstall using the option to configure as an application server.
The terminal server is not configured as a remote administration server.	Use the Add/Remove Programs tool to uninstall terminal servers, and then reinstall using the option to set up as a remote administration server.
A user's session is hung or the user cannot log off.	Open the Terminal Services Manager, right-click the user, and click Log Off.
You need to send a message to a user.	Open the Terminal Services Manager, right-click the user, click Send Message, enter the message, and click OK.
A user cannot run a program correctly.	The program is likely to have been installed before terminal services were installed. Remove the program and reinstall it.
No one can access the terminal server.	The server is disconnected or is not active. Open Terminal Services Manager, right-click the server, and click Connect to connect the server. Use the Terminal Services Licensing tool to activate server licenses.

Configuring a Telnet Server

Another way for clients to access resources on a Windows 2000 server is to use Telnet. Telnet is particularly useful for non-Windows clients such as IBM AS/400, some versions of UNIX, and others that support Telnet but that cannot access a Windows 2000 server as a terminal services client. As you learned in Chapter 3, Telnet is part of the TCP/IP application suite that enables a client to act as a terminal to access a server. Telnet is a technology that is almost as old as TCP/IP and is a TCP/IP application used to set up one computer as a network host and other computers as clients. Instead of running Windows-based terminal services, the client runs TCP/IP-based Telnet and accesses the Windows 2000 server, which is set up as a Telnet server instead of a Microsoft terminal server. The access is accomplished in a character-based mode and requires two elements: the Telnet Server service running on Windows 2000 Server, and Microsoft Telnet client or some other version of Telnet on the client computer. Also, the server and client must be configured for TCP/IP prior to running either Telnet Server or the client software. When a user telnets to a server, he or she must have a user account and supply the account name and password. Telnet can use NTLM authentication

(see NT LAN Manager in Chapters 4 and 7) to protect access to the server, but you must first turn on NTLM from the client (by entering the *NTLM* command in Telnet, if the client supports NTLM). Once connected, the user can execute programs and processes on the server for which that user has permissions. Telnet Server supports up to 63 clients.

The Windows 2000 Server Telnet Server service is started in one of two ways (on a server that is already configured to use TCP/IP). To use the first way:

1. Open the Computer Management tool and double-click Services and Applications.
2. Click Services under the tree.
3. Scroll the right-hand pane to find Telnet, right-click the service, and click Properties.
4. Click the Start button to start the service. If you plan to have the service running all of the time, set the Startup type box to Automatic. Click OK.

The second way to start the service is to open the Command Prompt window, enter *net start tlntsvr*, and press Enter.

The client computer must have Telnet installed—Windows 2000 Telnet client, for example. The Windows 2000 Telnet client is started from the Command Prompt window. To find out about Telnet commands, enter *telnet /?* in the Command Prompt window; to connect to a server, enter *telnet* and the name of the host computer, such as *telnet Lawyer*. To disconnect from a server, enter *exit* (or *quit* on some systems). When a Windows 2000 user starts Telnet and connects to the server, he or she views a command prompt window that is very similar to the same window on the client, but that window is actually on the server. On other systems, such as UNIX, Telnet may simply consist of command-line operations without a full-screen command window.

Windows 2000 Server out of the box is licensed to use only two simultaneous Telnet connections. More licenses are available when you purchase the add-on pack for Microsoft Windows Services for UNIX.

There are several different versions of Telnet client software. Make sure that users who telnet into a Telnet server check to make sure that they have set a password on the client side, or else intruders can telnet into their computers.

Installing a NetWare Gateway

On a network that combines use of NetWare servers and Windows 2000 servers, you may need to create a way for users to access a NetWare server through a Windows 2000 server that acts as a gateway. This is accomplished by installing **Gateway Service for NetWare**

(**GSNW**) in a Windows 2000 server. Used in this context, *gateway* means that the server acts as a go-between for Windows-based workstations and a NetWare file server. The workstations do not need to be NetWare clients, because they access the directories and files through the gateway, which appears to them as just another shared Windows 2000 server folder.

To install Gateway Service for NetWare, use the following general steps:

1. Create an account on the NetWare server for the Windows 2000 server to access (using SYSCON or NWADMIN). The appropriate directory and file attributes and access rights or group membership should be granted to the account, as determined by which directories and files will be made available for the users. For example, the NetWare account might be granted Read and File Scan access rights, which enable users to read files, run programs, and view file and subdirectory names.
2. Create a group on the NetWare server called NTGATEWAY, which has access rights to the files and directories that need to be used.
3. Make the NetWare user account a member of the NTGATEWAY group.

There are two places from which to control access to NetWare resources offered by a gateway. You can set up security through the access rights on the NetWare server, or you can set up security using share permissions on the Windows 2000 server. If you set up security in both places, keep in mind that the Windows 2000 server's gateway access is first restricted by the NetWare access rights and that user access is next restricted by the Windows 2000 Server share permissions.

4. Create a corresponding account on the Windows 2000 server.
5. Make sure that the appropriate protocol is installed in Windows 2000 Server for connecting to the NetWare server, such as NWLink or TCP/IP (see Chapters 3 and 6).
6. Install Gateway Service for NetWare on the Windows 2000 server by opening the Network and Dial-up Connections tool, right-clicking Local Area Connection, clicking Properties, and clicking the Install button. Double-click Client and then double-click Gateway (and Client) Services for NetWare.
7. If you see the Select NetWare Logon dialog box to designate a preferred NetWare server, you can enter that information now or configure it later as described in the next paragraphs. If you configure it now, enter the name of the Preferred Server and its associated information and then click OK. Or, click Cancel and then Yes, if you choose to configure the information later.
8. Click Yes to restart the Windows 2000 server.

After the Gateway (and Client) Services for NetWare are loaded, a new GSNW icon is added to the Control Panel. The GSNW icon enables you to configure the gateway, for instance

establishing a path to the NetWare server directories that will be offered as shared directories to clients. The steps for configuring the gateway are as follows:

1. Open the GSNW icon on the Control Panel, and click the Gateway button.
2. Click Enable Gateway.
3. Enter the NetWare account name, password, and password confirmation.
4. Click Add to create a shared folder.
5. Enter the share name, path to the NetWare server, drive, and user limit.
6. Click OK.
7. Set the share permissions.
8. Click OK.
9. Close the GSNW utility.

You can create multiple shared folders to different NetWare drives or directories by using the Add button and specifying a different share name, network path, and drive letter each time. When you configure the gateway, you have the option of specifying a preferred server or a default tree and context. A preferred server is the NetWare server that the gateway accesses by default, and that authenticates the logon. The tree and context option is used when the NetWare environment supports NetWare Directory Services, and it refers to the user account object and directory tree that are set by default.

When you install Gateway Service for NetWare, there also is an option to set default options for print queues that are accessed through the gateway. The print options are as follows:

- Add a form feed to each printout to make sure the last page prints
- Send a notification to users when a job has printed
- Print a banner page with each print job

There also is an option to run a login script on the NetWare server each time the gateway account logs on. The login script is a text script similar to Windows 2000 Server's logon script, containing commands that automatically run, such as specifying the operating system, account name, and other information. The preferred server, tree and context, print, and login script options are set from the Gateway Service for NetWare dialog box that appears when you first open the GSNW icon.

If you are troubleshooting a problem with connecting through Gateway Service for NetWare, start by using the *net* command to make sure that the service is working. Open the Command Prompt window, type *net view /network:nw*, press Enter, and look for a list of NetWare servers. If you see servers displayed, the gateway is working. If you do not see a list of NetWare servers, enter *net start "gateway service for netware"* in the Command Prompt window, and then use the *net* command to list the NetWare servers.

After Gateway Service for NetWare is installed, you can connect to NetWare print queues (the same as Windows 2000 Server shared printers) by using the Add Printer Wizard. To connect to NetWare printers for sharing on a Windows 2000 Server network:

1. Click Start, point to Settings, and click the Printers folder.
2. Double-click Add Printer, and click Next after the wizard starts.
3. Click Network printer and click Next.
4. Click *Type the printer name*, and enter the name of the NetWare printer in UNC format (*\\server\printer* in the Name box). Click Next.
5. Click Yes to print a test page, and click Next.
6. Click Finish.
7. Right-click the newly added printer in the Printers folder, click Sharing, and set up the printer to be shared. Also, if the Active Directory is installed, use the Active Directory Users and Computers tool to publish the printer (see Chapter 11).

CHAPTER SUMMARY

- A Windows 2000 server can be turned into a Web server through the installation of Internet Information Services (IIS). IIS comes with a range of tools that enables you to configure it for Internet Web access, to act as a media server, as an intranet server, and as a Web-based server for a VPN.
- Three other options for configuring a Windows 2000 server are as a DNS server to provide computer name and IP address resolution for a network, as a WINS server for NetBIOS-name-to-IP-address resolution, or as a DHCP server to lease IP addresses to network hosts.
- Providing terminal services is yet another function that a Windows 2000 server can perform. Terminal services involve using one of two modes: to enable remote access for server administrators to manage network servers, and to enable clients, such as thin clients, to run applications on the server.
- For clients that cannot use Windows 2000 terminal services, there is also the option to set up a Windows 2000 server as a Telnet server. Telnet is part of the TCP/IP application suite and is used to enable clients to emulate terminals on a computer set up as a Telnet server.
- Interoperability is important for enterprise networks that include Novell NetWare servers. Windows 2000 Server can be configured as a gateway to NetWare so that NetWare resources, such as directories and printers, appear as shared Windows 2000 Server resources.

In the next chapter, you learn how to monitor Windows 2000 Server, which is a first step in learning to pinpoint and diagnose problem areas, such as the need to add more RAM. You also learn how to tune and optimize server services and server performance.

KEY TERMS

DNS Server — A Microsoft service that resolves computer names to IP addresses, for example, resolving the computer name Brown to IP address 129.77.1.10, and that resolves IP addresses to computer names.

forward lookup zone — A DNS zone or table that maps computer names to IP addresses.

Gateway Service for NetWare (**GSNW**) — A service included with Windows NT and Windows 2000 Server that provides connectivity to NetWare resources for Windows NT and Windows 2000 servers and their clients, with the Windows NT or Windows 2000 server acting as a gateway.

host address (**A**) **resource record** — A record in a DNS forward lookup zone that consists of a computer name correlated to an IP version 4 address.

Internet Information Services (**IIS**) — A Microsoft Windows 2000 Server component that provides Internet Web, FTP, mail, newsgroup, and other services, and particularly the ability to set up a Web server.

Internet Server Application Programming Interface (**ISAPI**) — A group of dynamic-link library (DLL) files that consists of applications and filters to enable user-customized programs to interface with IIS and to trigger particular programs, such as a specialized security check or a database lookup.

Network News Transfer Protocol (**NNTP**) — A TCP/IP-based protocol used by NNTP servers to transfer news and informational messages to client subscribers who compose "newsgroups."

Open Database Connectivity (**ODBC**) — A set of rules developed by Microsoft for accessing databases and providing a standard doorway to database data.

pointer (**PTR**) **resource record** — A record in a DNS reverse lookup zone that consists of an IP (version 4 or 6) address correlated to a computer name.

reverse lookup zone — A DNS server zone or table that maps IP addresses to computer names.

scope — A range of IP addresses that a DHCP server can assign to clients.

Secure Sockets Layer (**SSL**) — A dual-key encryption standard for communication between an Internet server and a client.

streaming — Playing a multimedia audio, video, or combined file received over a network before the entire file is received at the client.

terminal — A device that consists of a monitor and keyboard, used to communicate with host computers that run the programs. The terminal does not have a processor to use for running programs locally.

terminal server — A server configured to offer terminal services so that clients can run applications on the server, which is similar to having clients respond as terminals.

thin client — A specialized personal computer or terminal device that has a minimal Windows-based operating system. A thin client is designed to connect to a host computer that does most or all of the processing. The thin client is mainly responsible for providing a graphical user interface and network connectivity.

Uniform Resource Locator (**URL**) — An addressing format used to find an Internet Web site or page.

virtual directory — A URL-formatted address that provides an Internet location (virtual location) for an actual folder on a Web server that is used to publish Web documents.

Web browser — Software that uses HTTP to locate and communicate with Web sites and that interprets HTML documents, video, and sound to give the user a sound and video GUI presentation of the HTML document contents.

Review Questions

1. Your company has set up a Web server to publish special promotions that have expiration dates. The marketing group is asking you if IIS has features to help with causing promotional Web files to expire after a certain number of days. How might this be possible?
   a. Configure the Operators default Web site properties to issue an alert to Web operators when files need to be deleted.
   b. Set up multiple Web publishing folders containing information that expires at the same time. Manually delete a folder on its expiration date.
   c. Create a Web-based spreadsheet showing when promotions expire and what files need to be deleted. Delete the files on the basis of the spreadsheet each morning.
   d. Configure the HTTP Headers default Web site properties to expire documents.
2. Your Web server users are calling to complain that FTP does not work, because they cannot use it to download files. How might you troubleshoot this problem?
   a. Check the permissions on FTP folders for those users.
   b. Install Media Services, which are required for FTP activity on an IIS server.
   c. Make sure that the FTP Publishing service is started.
   d. all of the above
   e. only a and b
   f. only a and c
3. You have set up a Web server, and now your users are asking for a better way to publish their Web pages than to hand-carry them to your office for you to install on the server. Which of the following will make you and them more productive?
   a. Create one or more virtual directories.
   b. Install Web services on all of their client computers and make pointers from the Web server to the clients.
   c. Configure Dfs for Web-only publishing.
   d. There is no more efficient way for users to publish Web pages.

4. You are in a planning meeting to set up a new network that will have Internet access, one Windows 2000 Web server, and four Windows 2000 servers for general file and printing access. Many of the clients are still using Windows 95 and NetBIOS applications. The organization for which you are planning has decided to implement the Active Directory. Which of the following should they include in their planning?
   a. Make at least two of the Windows 2000 servers domain controllers (DCs).
   b. Make at least two of the Windows 2000 servers DNS servers.
   c. Make at least one of the Windows 2000 servers a WINS server.
   d. all of the above
   e. only a and b
   f. only b and c
5. You are planning to implement a Web server that will also handle Internet e-mail services in conjunction with Microsoft Exchange service. Which of the following services enables you to transport e-mail over the Internet?
   a. SMTP
   b. NNTP
   c. FTP
   d. PPTP
6. You have configured DHCP to automatically update DNS servers, but the problem is that old leases are sometimes not removed or updated in the DNS servers. This is causing some mismatched IP resolutions. What can you do to solve the problem?
   a. This problem is most common on large networks, and you must disable automatic updating.
   b. This problem is caused by using TCP with IP on the network, and you must convert DNS servers to instead use UDP with IP.
   c. You need to configure DHCP to discard lookup records when their leases expire.
   d. You need to set leases so that they don't expire for a longer period of time.
7. You are the server administrator for a company and are on call several evenings a week to handle problems that may occur. Unfortunately, you live about 40 minutes from work and often have to go in to work in the evenings for tasks that only take a couple of minutes. How can you make your life easier by accessing administrative programs from home?
   a. Configure a terminal server as an application server.
   b. Configure a terminal server as a remote administration server.
   c. Configure a terminal server as a thin client.
   d. Unfortunately, there is no way to administer Windows 2000 servers from home.

8. Which of the following are IIS components that can be installed in Windows 2000 Server?
   a. Visual InterDev RAD Remote Deployment Support
   b. Common Files
   c. NNTP Service
   d. all of the above
   e. only a and b
   f. only a and c
9. One of your terminal services clients on a Windows 2000 server is having trouble with a client/server program that he runs. How might you help diagnose the problem?
   a. Lengthen the session timeout.
   b. Observe his keystrokes by connecting to view his session.
   c. Observe the applications he is using through the Command Prompt *Window* command.
   d. Restart the client/server program at the server.
10. One of your colleagues who works for another company is testing a Microsoft IIS Web server, but is concerned because there isn't better file security, such as the ability to designate one folder for read access to one group and another folder for read and write access by another group. What would you suggest?
    a. Use folder and file attributes for security.
    b. Configure the drive containing the Web files for NTFS, because as it now stands he has configured it for FAT, which has less security.
    c. Set up a VPN to configure security for general Web server access.
    d. all of the above
    e. only a and c
    f. only b and c
11. When you create a DNS server, what type of record will you most likely find in a reverse lookup zone?
    a. pointer resource record
    b. IPv6 host address (AAAA) resource record
    c. host address (A) resource record
    d. reverse host (R) resource record
12. Which of the following is(are) installed through the Add/Remove Programs tool as a Windows software component?
    a. IIS
    b. DHCP
    c. Terminal Services

d. all of the above

e. only a and b

f. only a and c

13. You have installed a counter on your e-commerce Web site and determined that it handles about 22,000 to 40,000 hits a day. This is a lot of traffic, and the Web site seems sluggish. Which of the following should you try first?

    a. Install more RAM.

    b. Set the foreground applications to get the most CPU time.

    c. Tune the Web server performance parameter from fewer than 10,000 hits to fewer than 100,000 hits.

    d. Decrease the page file size to reduce the amount of disk writing.

14. How can you make a client installation disk for a Terminal Services Windows 3.11 client?

    a. Use the Active Directory Users and Computers tool.

    b. Use the Terminal Services Client Creator tool.

    c. Use the Terminal Services Configuration tool.

    d. Terminal Services does not support Windows 3.11.

15. You have set up a Web server and now the management in your company wants to use it for multimedia training presentations. You have installed media services to prepare the server for this purpose. However, when you access a training film from the server at your workstation, it seems to take an unbearably long time to load before it starts playing. What should you do?

    a. Set up to use the streaming mode.

    b. Only purchase multimedia presentations that employ unicasting.

    c. Configure to use strongest encryption for fastest network access of multimedia.

    d. Make sure that no training file is larger than 1 MB, because this is a limitation for media services.

16. You have set up a TCP/IP-based Windows 2000 terminal server, and a user calls because she is trying to use the service for the first time by dialing in from home, but is not succeeding. What should she check?

    a. that her home computer is configured for TCP/IP

    b. that her home computer is set for full duplex

    c. that her home computer is configured for PPP

    d. all of the above

    e. only a and b

    f. only a and c

17. You are setting up a DHCP scope in which all of the clients are portable computers. For how long should you establish leases?
    a. one to two months
    b. seven days
    c. three to four days
    d. 8 to 24 hours
18. You have set up a Web server, created a virtual directory, and established the appropriate permissions for Web folders. After you release the server to users so that they can publish their own documents, many report some incompatibilities with using Microsoft FrontPage. Which of the following might be the problem?
    a. A special FrontPage FP permission must be assigned to the Web folders in which clients publish.
    b. The Web server IP address configuration tab has a FrontPage Extensions parameter that must be enabled so that it will authorize uploading FrontPage files from a client.
    c. FrontPage 2000 Server Extensions are not loaded as an IIS component.
    d. all of the above
    e. only a and c
    f. only b and c
19. Your network consists of 20 Windows 2000 servers and one older NetWare server that is using IPX/SPX communications. There are about 40 people who periodically access the NetWare server, but only at the rate of about four or five people at a time. What is the best way to access the NetWare server?
    a. Configure all clients to use RSVP to periodically reserve time on the NetWare server.
    b. Install Gateway Service for NetWare on one of the Windows 2000 servers for the clients to access.
    c. Configure the NetWare and Windows 2000 servers to use NetBEUI for common access.
    d. Use Windows 2000 Server terminal services for clients to access the NetWare server.
20. Your boss has worked on computer systems that support the use of a hashing algorithm for security, and she prefers this method. Can IIS Web security be configured for this security method?
    a. yes, by configuring it to use integrated Windows authentication
    b. yes, by configuring it to use basic authentication
    c. yes, by configuring it to use digest authentication
    d. A Web server does not support hashing for authentication.

21. When you are planning the installation of a DNS server, which of the following is(are) important to include in your planning?
    a. The DNS server should have a static IP address, not one assigned by DHCP.
    b. The DNS server should have an IP address that ends in "1," such as 129.70.88.1, because it must be the first server seen on the network.
    c. The DNS server must also be a DC.
    d. all of the above
    e. only a and b
    f. only a and c
22. Users are not able to access your Web server, and when you try it from your office, you cannot access it either. Which of the following might you do?
    a. Use the Internet Information Server management tool to restart IIS.
    b. Make sure that the Server service is started and running.
    c. Take the WINS server offline, because WINS can interfere with network access to IIS.
    d. all of the above
    e. only a and b
    f. only a and c
23. Which of the following are permissions used for Terminal Services?
    a. Full Control
    b. Write
    c. Execute
    d. all of the above
    e. only a and b
    f. only b and c
24. The Research group in your organization is setting up a Web server for a VPN that must have very restricted access. In a committee meeting, they ask you to list methods that can be used to restrict access. Which of the following is(are) possible?
    a. Restrict access by individual user IP address.
    b. Restrict access by IP subnet.
    c. Restrict access by domain.
    d. all of the above
    e. only a and b
    f. only b and c

25. You have installed Terminal Services, and several clients have called to say that Microsoft Word is not working properly. What should you do to solve the problem?
    a. Increase the channel bandwidth, because Microsoft Word requires more bandwidth.
    b. Reinstall Microsoft Word, because it was installed prior to installing Terminal Services.
    c. Increase the Terminal Services buffer used at those clients.
    d. all of the above
    e. only a and b
    f. only b and c

HANDS-ON PROJECTS

Project 13-1

In this project, you install Internet Information Services to set up a Web and FTP site.

To install IIS:

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click **Add/Remove Programs**, and click **Add/Remove Windows Components** (you may need to click the **Components** button next).
3. Find and then double-click **Internet Information Services (IIS)** in the Windows Component Wizard dialog box. What services are checked by default? Note these in your lab journal or in a word-processed document.
4. Make sure the following services are checked: **Common Files**, **Documentation**, **File Transfer Protocol Server (FTP)**, **FrontPage 2000 Server Extensions**, **Internet Information Services Snap-in, Internet Services Manager (HTML)**, and **World Wide Web Server**. Click **OK**.
5. Make sure that the box for **Internet Information Services (IIS)** is checked and has a gray background (the gray background in the box means that not all possible IIS services will be installed, only the ones you have checked in Step 4). Click **Next**.
6. If requested, insert the Windows 2000 Server CD-ROM and click **OK**. Also, if requested, provide the path to the CD-ROM and the \I386 folder. Click **OK**.
7. Click **Finish**.
8. Close the Add/Remove Programs tool, if it is still open.

Project 13-2

In this project, you set up a virtual directory from which to publish documents for the IIS Web server that you set up in Hands-on Project 13-1. Before you start, create a folder called Web Documents with your initials at the end of the folder name, for example Web DocumentsMJP.

To create a virtual directory:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Internet Services Manager**.
2. In the tree, click the name of the server on which you installed IIS in Hands-on Project 13-1, for example **Lawyer**.
3. Right-click **Default Web Site** in the right pane, point to **New**, and click **Virtual Directory** (Figure 13-19).

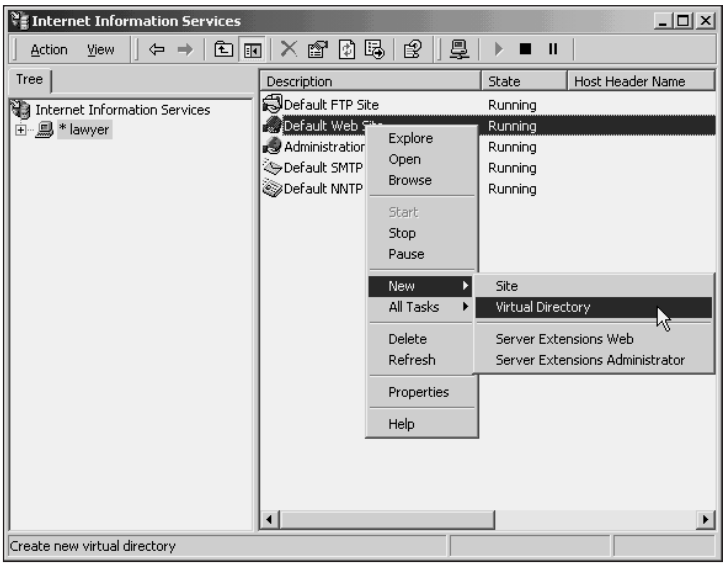

Figure 13-19 Creating a virtual directory

4. Click **Next** after the Virtual Directory Creation Wizard starts.
5. Enter an alias for the virtual directory, which users will employ to access it—for example, Webdocs plus your initials at the end, like this: **WebdocsMJP**. Click **Next**.
6. Enter the path to the actual folder you created before starting this assignment, for example **C:\Web DocumentsMJP**. Click **Next**.
7. What security options are available for you to set? What options would you need to set to enable users to copy HTML documents to the virtual directory? Similarly, how would you provide to users access only to read, browse, and view the source code for scripts? Record your observations in your lab journal or in a word-processed document.

8. Make sure that the options for **Read** and **Run Scripts** are checked; check these options if they are not selected. Also, check **Browse**. Click **Next** after you have configured the security options.
9 Click **Finish**.
10. How would you use the Internet Information Services tool to view the properties of the new virtual directory? Record your answer. Leave the Internet Information Services tool open for the next project.

Project 13-3

Assume that the Web site that you installed and configured in Hands-on Projects 13-1 and 13-2 is to be used for a VPN. You want to restrict access to users on the subnet 122.44.5 and to five users whose IP addresses are 122.44.10.22, 189.80.17.252, 189.80.19.40, 122.44.34.8, and 122.44.15.142.

To set up the IP restrictions:

1. Display the Web server, such as Lawyer, in the tree, and display its child objects to include Default Web Site.
2. Right-click **Default Web Site** and click **Properties**.
3. Click the **Directory Security** tab.
4. Click the **Edit** button in the IP address and domain name restrictions area of the tab.
5. Click **Denied Access** so that no IP addresses but those that you specify can access the Web site.
6. Click the **Add** button and click **Single computer**. How would you find an IP address, if you did not know it in advance? Record your observation. Enter the IP address **122.44.10.22** and click **OK** (refer to Figure 13-6). How would you enter the other four IP addresses? Enter each of the other addresses.
7. Back in the IP Address and Domain Name Restrictions dialog box, click the **Add** button and click **Group of computers**. Enter **122.44.5.0** for the network ID and **255.255.255.0** for the subnet mask, and then click **OK**. How would you enter additional subnets?
8. How would you restrict access to a domain? Record your answer.
9. Click **OK** to close the IP Address and Domain Name Restrictions dialog box, and click **OK** again.

Project 13-4

In this project, you learn how to install Windows Media Services and the Windows Media Services Administrator. An IIS Web server must already be installed before you begin.

To install Windows Media Services and the Administrator:

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click **Add/Remove Programs**, and click **Add/Remove Windows Components** (you may need to click the **Components** button next).

3. Find and then double-click **Windows Media Services** in the Windows Component Wizard dialog box.
4. Check the box for **Windows Media Services**. What happens to the **Windows Media Service Admin** box? Click **OK**.
5. Back in the Windows Components Wizard box, click **Next**.
6. If requested, insert the Windows 2000 Server CD-ROM and click **OK**. Also, if requested, provide the path to the CD-ROM and the \I386 folder. Click **OK**.
7. Click **Finish**.
8. Close the Add/Remove Programs tool, if it is still open.
9. Open the newly installed Windows Media Services Administrator by clicking **Start**, pointing to **Programs**, pointing to **Administrative Tools**, and clicking **Windows Media**. How would you determine if there is an equivalent MMC snap-in? Record whether there is a snap-in.
10. Notice the configuration options in the left pane, and note the options in your lab journal or in a word-processed document. What options are available to find out more about Windows Media Services?
11. Close the Windows Media Services Administrator.

Project 13-5

In this activity, you practice using the DNS management tool to create a record in the forward lookup zone. Also, you check for subfolders in the reverse lookup zone. Before you start, obtain from your instructor the name of a computer to add and its IP address. DNS should be previously installed on the computer that you use for practice.

To create a forward lookup zone record:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **DNS**.
2. In the tree, double-click **DNS**, double-click the computer name of the DNS server, double-click **Forward Lookup Zone**, and double-click the domain, such as **thefirm.com**.
3. In your lab journal or in a word-processed document, note the entries that you see in the right-hand pane for hosts. What is the entry for the DNS server?
4. Display the domain in the tree, if it is not already displayed, by double-clicking **DNS**, the DNS computer name, and the domain name.
5. Right-click the domain, such as **thefirm.com**, and click **New Host**.
6. Enter the name of the host computer, such as **Caribou**, and its IP address, such as **129.70.10.50** in the New Host dialog box.
7. Check the box to **Create associated pointer (PTR) record** (refer to Figure 13-12).
8. Click **Add Host** and click **OK** to confirm the creation of the new record.
9. Click **Done**.

To explore the reverse lookup zone:

1. Double-click **Reverse Lookup Zone** to display its child objects.
2. What reverse lookup zones exist for the DNS server?
3. How would you create a new zone?
4. Double-click a zone to display the folders under it for subnets. How would you create a new folder?
5. Double-click one of the folders, such as **10**.
6. What entries exist in the folder? Record the entries in your lab journal or in a word-processed document.
7. Right-click a folder and click **New Pointer**. What information do you need to enter to create a PTR record? Click **Cancel**.
8. Close the DNS management tool.

Project 13-6

In this project, you practice configuring a scope in DHCP and authorizing the server. The DHCP network services Windows component should be installed before you begin. Also, obtain the address or computer name of a DNS server from your instructor (your instructor may further want to provide you with a range of addresses for the scope and an address to exclude from the scope, but if not, use the addresses suggested in the project).

To configure DHCP:

1. Log on as Administrator or as a member of Enterprise Administrators.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **DHCP**.
3. Double-click **DHCP** in the tree, if the DHCP server name is not already displayed.
4. Right-click the DHCP server, such as **lawyer.thefirm.com [129.70.10.1]**, and click **New Scope**.
5. Click **Next** after the New Scope Wizard starts.
6. Enter a name for the scope to make it easy to identify as you maintain it—for example, **Manufacturing**—and enter a description for the scope, such as **Manufacturing building subnet**. Click **Next**.
7. Enter the start and end IP addresses, such as **129.70.19.51** and **129.70.19.99**. Further, enter the subnet mask, such as **255.255.255.0**, and then click the entry area in the Length box. What happens when you click the box? Click **Next**.
8. Enter the address **129.70.19.70** in the Start IP address box, and click **Add**. What happens after you click Add? Do you need to enter an ending address? Record your observations. Click **Next**.
9. What is the default lease time? For what types of situations would this default be appropriate? Record your answers. Change the default lease time to **4** days. Click **Next**.
10. Click **Yes, I want to configure these options now**, and click **Next**.

11. What information would you enter in the next dialog box, and why would you enter it? Click **Next**.
12. Enter the parent domain in which DNS name resolution will occur, such as **thefirm.com**. Enter the name of the DNS server obtained from your instructor, and click **Resolve**, or enter the DNS server's IP address. Click **Add**. How would you enter more than one DNS server? Click **Next**.
13. What information can you enter in the next dialog box, and why would you enter it? Click **Next**.
14. Click **Yes, I want to activate this scope now**, and then click **Next**.
15. Click **Cancel**, or if you have permission from your instructor to create the scope, click **Finish**.

To authorize a DHCP server:

1. Right-click the DHCP server, such as **lawyer.thefirm.com [129.70.10.1]**.
2. Click **Authorize**.
3. Does the status column change? If so, what does it say? Record your observations.
4. If the status column does not change, right-click the DHCP server, and click **Refresh**.
5. Right-click the server again, and click **Properties**.
6. Click the **DNS** tab. Is the server set up to update DNS lookup records? Will the default setup enable Windows 98 clients to update the DNS lookup records? Click **Cancel**.
7. Close the DHCP management tool.

Project 13-7

In this project, you set Terminal Services security in Windows 2000, and you create an installation disk for a Windows 98 client. Terminal Services should already be installed on the computer running Windows 2000 Server, and you will need to have two blank, formatted floppy disks.

To set the Terminal Services security:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Terminal Services Configuration**.
2. In the tree, double-click **Terminal Services Configuration**, if the Connections and Server Setting folders are not displayed.
3. Click **Connections**. What connections are displayed in the right-hand pane? Record your observations.
4. Double-click the connection, such as **RDP-Tcp**.
5. Click the **General** tab, if it is not displayed. What encryption level is set?
6. Click the arrow to list the options in the Encryption level box. What options do you see? Record your observations. Select **Medium**.
7. Check the box **Use standard Windows authentication**.

8. Click the **Permissions** tab.
9. Make sure the **Allow** boxes are checked for **Full Control**, **User Access**, and **Guest Account** for the **Administrators** group. How would you add a group and give it permissions?
10. Click **OK** and close the Terminal Services Configuration tool.

To create a client installation disk for Windows 98:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Terminal Services Client Creator**.
2. Click **Terminal Services for 32-bit x86 windows**. Make sure that the destination drive is A:, and click **OK**.
3. Insert the first floppy disk and click **OK**.
4. When you are prompted, remove the first disk, insert the second disk, and click **OK**.
5. Click **OK** after the files are copied to the second disk. What would you do next to install the software in Windows 98?

CASE PROJECTS

Aspen Consulting Project: Configuring Interoperability

Brighton Community College is designing and implementing a new network that primarily consists of Windows 2000 servers. They have purchased 10 server computers that will run Windows 2000 Server. The campus will have Internet access and will offer a Web server on the Internet. They also plan to set up DNS and DHCP servers for the network. Currently, they have a small network that has two older NetWare servers running NetWare version 4.1. The college has hired you to work with their IT Department to plan and implement the new network.

1. Develop a document explaining to the IT Department how to plan the implementation of the Web, DNS, and DHCP servers. In that document, address the following issues, as well as others that you think are important:
   - In what order should the Web, DNS, and DHCP services be implemented for network use? Should all of these services be implemented on one server or on different servers?
   - What setup elements should be planned in advance, such as DHCP scopes, DNS lookup zones, and Web services? What factors should go into their planning?
   - What security issues should be addressed in the setup of these services?
2. The IT Department needs training in how to deploy a Web and FTP server. Create a general training document that explains the following:
   - How to install a Web and FTP server
   - How to set up a virtual directory
   - How to configure the Web server

3. The IT Department has now set up a Web and FTP server, but no one is able to access it. Work through different troubleshooting steps that they can follow to identify the problem.
4. The IT Department has set up a DNS server, but it has no reverse lookup zone. This prompts several questions about DNS setup:
   - What is the purpose of a reverse lookup zone, and how can it be set up?
   - Can more than one DNS server be configured when the Active Directory is deployed, and if so, what is the advantage?
   - Can DHCP be configured to automatically update DNS records, and if so, how?
5. The IT Department has installed DHCP and configured it, but for some reason it is not communicating on the network. What troubleshooting steps should it try in order to solve the problem?
6. The computer room in which the Windows 2000 servers are located is down the hall from the IT offices. How can the IT Department configure terminal services so that it can remotely administer the servers without going to the computer room? How can it set security to make sure that only the IT Department can access the servers?
7. Once all of the Windows 2000 servers are set up, the IT Department wants to set up access to directories on the NetWare servers so that NetWare access appears like any other shared Windows 2000 folder. How can it set up this type of access to the NetWare servers?

Optional Case Projects for Teams

Team Case One

Many of the Aspen consultants are not sure about all of the ways that Windows 2000 Server Terminal Services can be deployed to benefit an organization. Form a team and document four scenarios in which to use terminal services.

Team Case Two

Multimedia applications are growing in use via Web-based servers. Mark Arnez asks you to form a team to research three different kinds of multimedia Web applications and how to deploy them using Windows 2000 Server IIS.